世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6 **H04N 7/16, 7/167, 7/08, H04K 1/04, H04L 12/18**	**A1**	(11) 国際公開番号 **WO00/03541** (43) 国際公開日 2000年1月20日(20.01.00)

(21) 国際出願番号 PCT/JP98/03127

(22) 国際出願日 1998年7月13日(13.07.98)

(71) 出願人（米国を除くすべての指定国について）
ソニー株式会社(SONY CORPORATION)[JP/JP]
〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
窪田達也(KUBOTA, Tatsuya)[JP/JP]
若槻典生(WAKATSUKI, Norio)[JP/JP]
〒141-0001 東京都品川区北品川6丁目7番35号
ソニー株式会社内 Tokyo, (JP)
(74) 代理人
弁理士 田辺恵基(TANABE, Shigemoto)
〒150-0001 東京都渋谷区神宮前1丁目11番11-508号
グリーンフアンタジアビル5階 Tokyo, (JP)

(81) 指定国 JP, KR, US, 欧州特許 (CY, DE, FR, GB, IT, NL)

添付公開書類
国際調査報告書

(54)Title: **DATA MULTIPLEXER, PROGRAM DISTRIBUTION SYSTEM, PROGRAM TRANSMISSION SYSTEM, TOLL BROADCAST SYSTEM, PROGRAM TRANSMISSION METHOD, LIMITED RECEIVING SYSTEM, AND DATA RECEIVER**

(54)発明の名称 データ多重化装置、プログラム配信システム、プログラム伝送システム、有料放送システム、プログラム伝送方法、限定受信システム及びデータ受信装置

Program number	Video	Main Audio	Sub Audio	Private
1	Ks1		---	---
2	Ks2		Ks3	Ks4
3	Ks5	Ks6	---	---
4	Ks7	Ks8	Ks9	Ks10
5	Ks11			
6	Ks12		---	---
7	Ks13			Ks14
8	Ks15			
9	Ks16	Ks17	Ks18	Ks19

(57) Abstract

A data multiplexer, a program distribution system, a program transmission system, a toll broadcast system, a program transmission method, a limited receiving system, and a data receiver for transmitting transport stream packets of program data comprising a plurality of data elements having a transport stream packet structure, wherein a viewer can make a reception contract for each data element by generating a scramble key Ks corresponding to one or more data elements out of the data elements constituting one program and performing scrambling for each data element.

(57)要約

トランスポートストリームパケット構成の複数のデータエレメントからなるプログラムデータの各トランスポートストリームパケットを多重化して送信するデータ多重化装置、プログラム配信システム、プログラム伝送システム、有料放送システム、プログラム伝送方法、限定受信システム及びデータ受信装置において、１つのプログラムを構成する複数のデータエレメントのうち、１つ又は複数のデータエレメントに対応したスクランブルキーＫｓを生成し、各データエレメントごとにスクランブルをかけるようにすることにより、視聴者はデータエレメントごとに視聴契約を結ぶことができる。

明　細　書

データ多重化装置、プログラム配信システム、プログラム伝送システム、有料放送システム、プログラム伝送方法、限定受信システム及びデータ受信装置

技術分野

本発明はデータ多重化装置、プログラム配信システム、プログラム伝送システム、有料放送システム、プログラム伝送方法、限定受信システム及びデータ受信装置に関し、例えばビデオデータやオーディオデータを圧縮符号化し、多重化して伝送するデジタル放送システムのデータ多重化装置及びデータ受信装置に適用して好適なものである。

背景技術

近年、ＭＰＥＧ２（Ｍｏｖｉｎｇ　Ｐｉｃｔｕｒｅ　Ｅｘｐｅｒｔｓ　Ｇｒｏｕｐ　Ｐｈａｓｅ　２）を用いてビデオデータやオーディオデータを圧縮符号化し、その符号化されたストリームを地上波や衛星波を利用して放送するデジタル放送システムが提案されている。このデジタル放送システムは、符号化されたビデオストリーム及び符号化されたオーディオストリーム等から構成される複数の各プログラムについて、各プログラムのビデオデータやオーディオデータ等のエレメンタリデータを所定バイト単位で分割し、その分割された各データの先頭にヘッダを加えることにより複数のトランスポートパケットを生成する。そしてこのトランスポートパケットを多重化し、地上波や衛星波を利用して送信する。

受信装置では、トランスポートパケットを多重化してなる伝送データを受信すると、この受信されたデータから各トランスポートパケットのヘッダ情報を読出し、このヘッダ情報に基づいて多重化される前のエレメンタリデータを復元することにより、各プログラムの符号化されたビデオストリーム及び符号化されたオ

ーディオストリーム等を得る。

このようなデジタル放送システムにおいて、一般的に、1つのプログラムは複数のデータエレメント（ビデオデータと複数チャンネルのオーディオデータ）から構成されている。このようなデジタル放送システムにおいて、1つのプログラムの中に含まれるデータエレメント毎に、視聴者が契約を行うことが望まれている。例えば、1つのプログラムが、ビデオデータ、メインオーディオデータ、サブオーディオデータ、及び付加データ等の合計4つのデータエレメントから構成されている場合を想定する。従来のデジタル放送システムでは、1つのプログラム毎に契約を行っていた、つまり、6つのデータエレメント全てと契約しなければいけなかった。つまり、受信者がビデオデータとメインオーディオデータのみを契約したいと思っても、不必要な残りのエレメント（サブオーディオと付加データ）までも契約しなければいけないという問題があった。

また、従来のスクランブル装置は、多重化する前に行われていたので、プログラム毎のスクランブル装置が必要であり、装置の構成が大きくなる問題があった。

さらに、従来のデジタル放送システムでは、番組契約情報や暗号解読キーを一定の期間毎にプログラムに多重化して伝送していた。多重化されたストリームのビットレートの上限は制限されているので、番組契約情報や暗号解読キーを伝送する分だけ、プログラムの伝送レートを確保できない場合がある。伝送レートを十分海保できないときには、いずれかのプログラムデータをバッファリングする伝送バッファがオーバーフローしてしまうという問題を有していた。

発明の開示

本発明は、そのような点を鑑みてなされた発明であって、受信者がプログラムを構成するデータエレメントのうち必要なデータエレメントのみを受信できるような、つまり、データエレメント毎にスクランブルをかけることのできるデジタル放送システムを提案するものである。

また、本発明は、プログラム毎にスクランブル装置を設ける構成を回避して装置構成を小型化することのできるデジタル放送システムを提案するものである。

また、本発明は、いずれかのプログラムデータをバッファリングする伝送バッファのオーバーフローを回避し得るデジタル放送システムを提案するものである。

かかる課題を解決するため本発明においては、トランスポートストリームパケット構成の複数のデータエレメントからなるプログラムデータの上記各トランスポートストリームパケットを多重化して送信するデータ多重化装置において、データエレメントごとに対応するスクランブルキーを生成するスクランブルキー生成手段と、スクランブルキー生成手段によって生成されたスクランブルキーを用いて対応する上記データエレメントのトランスポートストリームパケットにスクランブルをかけるスクランブル手段とを備え、1つのプログラムを構成する複数のデータエレメントのうち、1つ又は複数のデータエレメントに対応したスクランブルキーを生成し、各データエレメントごとにスクランブルをかけるようにする。

各データエレメントごとにスクランブルをかけることにより、視聴者はデータエレメントごとに視聴契約を結ぶことができる。

また本発明においては、複数のデータエレメントから構成されるプログラムを配信するプログラム配信システムにおいて、プログラム毎及びデータエレメント毎の顧客の契約を顧客管理システムによって管理すると共に、プログラムに含まれるデータエレメントをデスクランブルする際に使用するスクランブルキーをデータエレメント毎に生成し、生成されたスクランブルキーに基づいて、多重化ストリームに含まれる符号化データエレメントに対して各データエレメント毎に選択的にスクランブルをかけることにより、視聴者は各データエレメント毎に視聴契約を結ぶことができる。

また本発明においては、複数のデータエレメントから構成されるプログラムを伝送するプログラム伝送システムにおいて、顧客が契約したプログラム及びデー

タエレメントのみを視聴できるように、プログラムに含まれる複数のデータエレメントをスクンブルする際に使用される複数のスクランブルキーを生成し、当該生成されたスクランブルキーに基づいて各データエレメント毎に選択的にスクランブルをかけ、当該スクランブルがかけられたデータエレメントを多重化して伝送することにより、視聴者は各データエレメント毎に視聴契約を結び、その契約されたデータエレメントのみをスクランブル解除して視聴することができる。

また本発明においては、複数のデータエレメントから構成されるプログラムを放送する有料放送システムにおいて、プログラム毎及びデータエレメント毎の顧客の契約を顧客管理システムによって管理すると共に、プログラムに含まれるデータエレメントをデスクランブルする際に使用するスクランブルキーをデータエレメント毎に生成し、生成されたスクランブルキーに基づいて、多重化ストリームに含まれる符号化データエレメントに対して各データエレメント毎に選択的にスクランブルをかけることにより、視聴者は各データエレメント毎に視聴契約を結ぶことができる。

また本発明においては、プログラム配信システムから配信された複数のプログラム及び当該プログラムを構成する複数のデータエレメントのうち、契約されたプログラム及びデータエレメントのみを限定的にち受信する限定受信システムにおいて、複数の暗号化スクランブルキーを含んだ複数のトランスポートストリームパケットから、受信者が契約したプログラム及びデータエレメントに関連付けられた暗号化スクランブルキーを含んだトランスポートストリームパケットをフィルタリングし、当該フィルタリングされた複数のトランスポートストリームパケットに含まれる複数の暗号化スクランブルキーの暗号を解読し、暗号解読された複数のスクランブルキーを生成し、複数のデータエレメントに対応付けられた複数の暗号解読されたスクランブルキーを使用して複数のデータエレメント毎にデスクランブルすることにより、視聴者は各データエレメント毎に視聴契約を結び、その契約されたデータエレメントのみをスクランブル解除して視聴することができる。

また本発明においては、多重化された各トランスポートストリームパケットに対してそれぞれ対応するスクランブルキーを用いてスクランブルをかけることにより、各トランスポートストリームパケットを多重化する前にスクランブルをかける場合に比べて、スクランブルをかけるための回路構成が簡単になる。

また本発明においては、複数のデータエレメントを構成する複数のパケットデータを格納する複数のバッファメモリと、バッファメモリを切り換えるスイッチ手段を有し、当該スイッチ手段によつてバッファメモリを順次時分割に切り換えることによって複数のパケットデータ列を時分割に多重化して出力する多重化手段と、スイッチ手段による切り換え対象である複数のバッファメモリを、パケットデータ列の入力レートに応じて選択するスイッチ制御手段とを備え、入力レートが基準レートに比べて高いとき、複数のバッファメモリのうち、優先順位の低い情報をバッファリングするバッファメモリを切り換え対象から除外してスイッチ手段を切り換え制御することにより、優先順位の高いデータエレメントをバッファリングするバッファメモリがオーバーフローすることを未然に防止し得る。

また本発明においては、トランスポートストリームパケット構成の複数のデータエレメントからなるプログラムデータの各トランスポートストリームパケットを多重化してなる多重化データを受信するデータ受信装置において、データエレメントごとに対応するスクランブルキーを多重化データから抽出するスクランブルキー抽出手段と、スクランブルキー抽出手段によつて抽出されたスクランブルキーを用いて多重化データに含まれる各データエレメントごとのトランスポートストリームパケットをデスクランブルするデスクランブル手段とを備え、スクランブルキーを用いて当該スクランブルキーに対応するデータエレメントごとにそのトランスポートストリームパケットをデスクランブルすることにより、データエレメントごとに個別にスクランブルを解除することができる。

図面の簡単な説明

図1は、本発明によるデジタル放送システムの構成を示すブロック図である。

図２は、各プログラムに含まれるエレメンタリデータとスクランブルキーとの対応を示す略線図である。

図３は、トランスポートストリームパケットに記録される情報とそのＰＩＤ値との対応を示す略線図である。

図４は、トランスポートパケットの種類とそのＰＩＤ値との対応を示す略線図である。

図５は、エンコーディイングシステムの構成を示すブロック図である。

図６は、トランスポートパケットのシンタックスを示す略線図である。

図７は、トランスポートパケットのシンタックスを示す略線図である。

図８は、トランスポートパケットのシンタックスを示す略線図である。

図９は、トランスポートパケットのシンタックスを示す略線図である。

図１０は、マルチプレクサシステムの構成を示すブロック図である。

図１１は、各テーブルとそのＰＩＤとの対応を示す略線図である。

図１２は、ｐｒｏｇｒａｍ　ａｓｓｏｃｉａｔｉｏｎ　ｓｅｃｔｉｏｎのシンタックスを示す略線図である。

図１３は、ｐｒｏｇｒａｍ　ａｓｓｏｃｉａｔｉｏｎ　ｓｅｃｔｉｏｎのシンタックスを示す略線図である。

図１４は、各セクションとそのＰＩＤ値との対応を示す略線図である。

図１５は、ｐｒｏｇｒａｍ　ｍａｐ　ｓｅｃｔｉｏｎのシンタックスを示す略線図である。

図１６は、ｐｒｏｇｒａｍ　ｍａｐ　ｓｅｃｔｉｏｎのシンタックスを示す略線図である。

図１７は、ｃｏｎｄｉｔｉｏｎａｌ　ａｃｃｅｓｓ　ｓｅｃｔｉｏｎのシンタックスを示す略線図である。

図１８は、ｃｏｎｄｉｔｉｏｎａｌ　ａｃｃｅｓｓ　ｓｅｃｔｉｏｎのシンタックスを示す略線図である。

図１９は、ｃｏｎｄｉｔｉｏｎａｌ　ａｃｃｅｓｓ　ｄｅｓｃｒｉｐｔｏｒのシンタックスを示す略線図である。

図２０は、各テーブルによって表されるエレメンタリデータのＰＩＤと、ｄｅｓｃｒｉｐｔｏｒの内容を示す略線図である。

図２１は、ＥＭＭパケットのデータ構成を示す略線図である。

図２２は、ＥＣＭパケットのデータ構成を示す略線図である。

図２３は、受信装置の構成を示すブロック図である。

発明を実施するための最良の形態

以下、図面について本発明の一実施例を詳述する。

図１を参照して、本発明のデータ多重化装置が適用されるデータ放送システムに関して説明する。

このデータ放送システムは、衛星デジタル放送システムや地上波デジタル放送システムなどの有料の放送システムにおいて使用されるシステムであって、図１に示すように、放送番組編成システムＢＤＰＳ（Ｂｒａｏｄｃａｓｔ＿Ｄａｔａ＿Ｐｒｏｃｅｓｓｉｎｇ＿Ｓｙｓｔｅｍ）１と、顧客管理システムＳＭＳ（Ｓｕｂｓｃｒｉｂｅｒ＿Ｍａｎａｇｅｍｅｎｔ＿Ｓｙｓｔｅｍ）２と、顧客視聴許可システムＳＡＳ（Ｓｕｂｓｃｒｉｂｅｒ＿Ａｕｔｈｏｒｉｚａｔｉｏｎ＿Ｓｙｓｔｅｍ）３と、ＥＰＧ（Ｅｌｅｃｔｒｏｎｉｃ＿Ｐｒｏｇｒａｍ＿Ｇｕｉｄｅ）システム４と、サーバシステム５と、ルーテイングシステム６と、エンコーディングシステム７と、マルチプレクサシステム８と、エンコーダ／マルチプレクサコントロールユニット９と、変調回路１０とから構成されている。

放送番組編成システム１は、顧客管理システム２、顧客視聴許可システム３、ＥＰＧシステム４、サーバシステム５、ルーテイングシステム６、エンコーディングシステム７、マルチプレクサシステム８、エンコーダ／マルチプレクサコントロールユニット９及び変調回路１０等の放送局に設けられている全てのシステム及び装置を統括的に管理するためのシステムである。この放送番組編成システ

ム１には、番組供給会社から供給された番組素材及びプロモーション素材や自局で作成した番組素材やＣＭ素材などのあらゆる素材の放映時間を管理するための番組編成表が登録されており、放送番組編成システム１は、この番組編成表に従って、各装置及びシステムを制御する。この番組編成表は、例えば、番組供給会社に関する情報などが記録されているサービス情報ファイル、１時間単位又は１日単位の放送番組スケジュールが記録されているイベント情報ファイル、及び１５秒単位の放送番組のタイムスケジュールが記録されている運行情報ファイル等から構成されている。

顧客管理システム２は、顧客登録情報や料金徴収情報等の顧客管理に関する情報を管理するためのシステムである。具体的には、この顧客管理システム２は、顧客の番組契約、課金、請求を中心とする有料放送システムの中核システムである。さらにこの顧客管理システム２は、データエレメントをスクランブルするためのスクランブルキーＫｓを暗号化するためのワークキーＫｗ等の鍵に関する情報や、委託放送事業者や番組供給会社や番組作成代理店の管理を行うための機能を有している。また、この顧客管理システム２は、受信側に設けられたＩＲＤから電話回線を通じて供給される視聴情報をリアルタイムに処理する機能を有している。また、この顧客管理システム２は、後述する顧客視聴許可システム３に対して、視聴者の契約に関する契約情報やワークキーＫｗに関する情報が格納されたＥＭＭ（Ｅｎｔｉｔｌｅｍｅｎｔ＿Ｍａｎａｇｅｍｅｎｔ＿Ｍｅｓｓａｇｅ）データを供給する。このＥＭＭデータについては詳しくは後述する。

顧客視聴許可システム３は、顧客管理システム２から受け取ったＥＭＭデータに含まれるワークキーＫｗを、マスタキーＫｍを使用して所定の暗号化アルゴリズムにて暗号化することによって、暗号化されたワークキーＫｗ’を生成する。尚、本発明のデジタル放送システムで用いられている暗号化アルゴリズムは、当社が開発した暗号化アルゴリズムＣＲＹＰＳ（ソニー登録商標）という暗号化アルゴリズムであって、米国商務省で定められたＤＥＳ方式と同じブロック暗号方式である。さらに、この顧客視聴許可システム３は、顧客管理システム２から供

給されたＥＭＭデータに含まれているワークキーＫｗを、暗号化アルゴリズムＣＲＹＰＳによって暗号化されたワークキーＫｗ’に置換え、新たな暗号化されたＥＭＭデータを生成する。また、顧客視聴許可システム３は、この当社独自の暗号アルゴリズムによって暗号化されたＥＭＭデータを衛星を介して伝送するために、この暗号化されたＥＭＭデータをトランスポートストリームパケットのペイロード部に挿入することによって、暗号化されたＥＭＭデータをトランスポートストリームパケットの形態に変換する。以下の説明において、このＥＭＭデータを含んだトランスポートストリームパケットをＥＭＭパケットと呼ぶ。尚、この顧客視聴許可システム３は、このＥＭＭパケットに付与されるＰＩＤ（パケット識別子）を、後述するエンコーダ／マルチプレクサコントロールユニット９からネットワークを介して受け取る。

さらに、この顧客視聴許可システム３は、２５６個のワークキー（Ｋｗ）とそのワークキーを識別するためのワークキー識別番号（Ｋｗ＿Ｎｏ）とを対応付けたワークキーテーブルを有しており、このワークキーテーブルをネットワークを介してマルチプレクサシステム８内のメモリにダウンロードする。このようなワークキーテーブルをマルチプレクサシステム８にダウンロードする理由は、この視聴許可システム３からマルチプレクサシステム８には暗号化されたワークキーＫｗ’しか伝送されないので、マルチプレクサシステム８においてワークキー識別番号（Ｋｗ＿Ｎｏ）から暗号化されていないワークキーｋｗを得るためである。

また、この顧客視聴許可システム３は、伝送されるプログラムに含まれる各データエレメントにスクランブルを施すためのスクランブルキーＫｓを生成する。顧客視聴許可システム３は、各プログラム毎又はプログラムに含まれる各データエレメント毎に異なるスクランブルキーＫｓを生成する。例えば、図２に示すように、第１のプログラムを構成するビデオデータ及びメインオーディオデータをそれぞれスクランブルするためのスクランブルキーとしてＫｓ１を生成し、第２のプログラムのビデオデータ及びメインオーディオデータをスクランブルするた

めのスクランブルキーとしてＫｓ２を生成し、第２のプログラムのサブオーディオデータをスクランブルするためのスクランブルキーとしてＫｓ３を生成し、第２のプログラムのプライベートデータをスクランブルするためのスクランブルキーとしてＫｓ４を生成する。どのプログラムのどのエレメントに対してどのようなスクランブルキーを割り当てるかは、プログラム内容に応じて顧客視聴許可システム３が自由に決定できる。例えば、第４のプログラムのように、ビデオデータ、メインオーディオデータ、サブオーディオデータ及びプライベートデータに対してそれぞれ異なるスクランブルキーＫｓ７～Ｋｓ１０を設定したり、又は、第５のプログラムのように、ビデオデータ、メインオーディオデータ、サブオーディオデータ及びプライベートデータに対してそれぞれ同じスクランブルキーＫｓ１１を設定したりするような自由な設定が可能である。

さらに、顧客視聴許可システム３は、このデジタル放送システムにおける暗号／暗号解読システムのセキュリティを高めるため、顧客視聴許可システム３の内部に設けられた乱数発生器によって、これらのスクランブルキーＫｓ１～Ｋｓ１９を４秒おきに更新している。

また、顧客視聴許可システム３は、スクランブルを解除するために使用される複数のＥＣＭ（Ｅｎｔｉｔｌｅｍｅｎｔ＿Ｃｏｎｔｒｏｌ＿Ｍｅｓｓａｇｅ）データを生成する。このＥＣＭデータは、ワークキーテーブルの中の少なくとも１つのワークキーＫｗを指定するためのワークキー番号、及びデータストリームに対してスクランブルをかけるためのスクランブルキーＫｓ、及び、この顧客視聴許可システム３を識別するためのＣＡ＿ｓｙｓｔｅｍ＿ID等のデータから構成されている。従って、１つのＥＣＭデータには、１つのスクランブルキーしか登録できないので、図２に示した１９個のスクランブルキーＫｓ１～Ｋｓ１９を使用する例においては、顧客視聴許可システム３は、１９個のＥＣＭデータを生成する。

さらに、顧客視聴許可システム３は、生成された複数のＥＣＭデータを伝送するために、この複数のＥＣＭデータをトランスポートストリームパケットのペイ

ロード部に挿入することによって、複数のＥＣＭデータをトランスポートストリームパケットの形態にそれぞれ変換する。以下の説明において、このＥＣＭデータを含んだトランスポートストリームパケットをＥＣＭパケットとして説明する。また、図１においては、スクランブルキーＫｓ１を含んだＥＣＭパケットをＥＣＭ１と記し、スクランブルキーＫｓ２を含んだＥＣＭパケットをＥＣＭ２と記し、以下同様にして、スクランブルキーＫｓ３～Ｋｓ１９を含んだＥＣＭパケットをそれぞれＥＣＭ３～ＥＣＭ１９と記している。尚、この顧客視聴許可システム３は、この複数のＥＣＭパケットに付与されるＰＩＤ（パケット識別子）を、後述するエンコーダ／マルチプレクサコントロールユニット９からネットワークを介して受け取る。また、図１には、ＥＣＭパケットが、直接マルチプレクサシステムに供給されるように記されているが、これはＥＣＭパケットの送出元及び送り先をわかりやすく示すためだけであって、実際には、ネットワーク及びエンコーダ／マルチプレクサコントロールユニット９を介してマルチプレクサシステム８に供給される。

次に、デジタル放送システムにおいて上述したワークキー及びスクランブルキーを使用する理由について説明する。

一般的なデジタル放送システムにおいては、番組視聴契約を行った特定の視聴者のみに視聴を許可すると共に、番組の契約内容に応じてその特定の視聴者に課金する有料放送システムが適用されている。このデジタル放送システムにおいて有料放送システムを実現するためには、放送局側で作成したスクランブルキーを使用して伝送すべきプログラムにスクランブルをかけ、番組視聴契約を行った特定視聴者のみがそのスクランブルを解除してプログラムを視聴できるようにしなければいけない。スクランブルが施されたデータエレメントを受信機側において特定視聴者のみが解読できるようにするためには、スクランブルする際に使用したスクランブルキーＫｓを使用することによってスクランブルを解除する必要がある。衛星を介して伝送されたプログラムのスクランブルを自動で解除するためには、このスクランブルキーＫｓを受信機側に伝送しなければいけない。

しかしながら、このスクランブルキーＫｓを受信機側に伝送してしまうと、番組契約していない視聴者がこのスクランブルキーＫｓを取得し、その結果伝送された全てのプログラムを無料で視聴できることになってしまう。よって、本発明の有料放送システムでは、第１のセキュリティとして、このスクランブルキーＫｓを、乱数発生器を使用して数秒単位で変更するとともに、ワークキーｋｗによって、このスクランブルキーＫｓを暗号化している。この乱数発生器を使用したスクランブルキーＫｓの暗号化は、ソフトウエアによって実現できるので、暗号強度としてはかなりセキュリティが高いといえる。

本発明のデジタル放送システムでは、さらに一層、限定受信システムのセキュリティを高めるために、このスクランブルキーＫｓを、マルチプレクサシステム８の後述する暗号化回路８２２においてワークキーＫｗを使用して暗号化し、暗号化したスクランブルキーＫｓ’を受信機側に伝送するようにしている。つまり、プログラムのスクランブルに使用したスクランブルキーＫｓをそのまま送るのでは無く、そのスクランブルキーＫｓ自体を暗号化して送ることによって、セキュリティを最大限にまで高めている。また、受信機側において、この暗号化されたスクランブルキーＫｓ’の暗号化を解くための解読器（Ｄｅｃｒｙｐｔｅｒ）は、受信機内のセキュリティモジュール（ＩＣカード）内に収められており、この暗号解読処理は全てこのセキュリティモジュール内部で行われる。このＩＣカードから構成されるセキュリティモジュールは、内部のプログラムコードを解読することは事実上不可能な構造とされ、従って、全く異なる第３者がこのスクランブルキーの暗号を解くことは極めて困難であるといえる。

ＥＰＧシステム４は、伝送されたプログラムに関連する番組ガイドデータを作成するためのシステムである。番組ガイドデータ（ＥＧＰデータ）とは、例えば、今後の放送予定のプログラムの放送時間の案内データ、指定された番組の内容を説明するための文字データ、番組のタイトルデータ等のデータのことである。このＥＰＧデータは、放送局が作成する場合が主であるが、プログラムをした番組供給会社が個別のＥＰＧデータを作成する場合もあり得る。

サーバシステム５は、各種素材が記録されたディスクドライブをアレイ状に接続することによって構成されたサーバと、このサーバの記録／再生動作を制御するためのサーバ制御用コンピュータとから構成されている。このサーバシステム５は、放送番組編成システム１とイーサネット等の局内のＬＡＮによって接続され、放送番組編成システムの番組編成リストに従ったプログラムを送出するように制御される。このサーバシステム５に記録されている素材は、例えば、ＣＭ素材を供給するためのＣＭサーバ機能、テレビ番組素材やニュース番組素材を供給するためのデイリーサーバ機能、及び、テレビ番組素材や映画素材を供給するためのビデオオンデマンド（ＶＯＤ）サーバ機能を有しており、放送番組編成システム１からの制御に基いて、任意のチャンネルに複数の任意のプログラムを出力することができる。

ルーティングシステム６は、サーバシステム５から供給された複数チャンネルのデータが適切なチャンネルから出力されるようにルーティングするためのシステムである。このルーティングシステム６は、放送番組編成システム１とイーサネットによって接続され、放送番組編成システムの番組編成リストに従ったプログラムを適切なチャンネルに送出するようにルーティング制御される。

エンコーダ／マルチプレクサコントロールユニット９は、エンコーディングシステム７及びマルチプレクサシステム８を制御するための制御コマンドを、ネットワークを介してエンコードシステム７及びマルチプレクサシステム８に供給する。エンコーダ／マルチプレクサコントロールユニット９は、ＥＰＧシステム４からネットワークを介してＥＰＧパケットを受け取ると共に、顧客視聴許可システム３からネットワークを介してＥＣＭパケット（ＥＣＭ１～ＥＣＭ１９）及びＥＭＭ’パケットを受け取り、受け取ったＥＰＧパケット、ＥＭＭ’パケット及びＥＣＭパケットをマルチプレクサシステム８に供給する。さらに、エンコーダ／マルチプレクサコントロールユニット９は、エンコーディングシステム７にプライベートデータを供給すると共に、マルチプレクサシステム８にプログラム仕様情報（ＰＳＩ：Ｐｒｏｇｒａｍ＿Ｓｐｅｃｉｆｉｃ＿Ｉｎｆｏｒｍａｔｉｏｎ

）を供給する。

プログラム仕様情報ＰＳＩは、指定されたプログラム番号とそのプログラム番号に対応するプログラムマップテーブル（ＰＭＴ）のトランスポートストリームパケットを指し示すためのプロブラムアソシエーションテーブル（ＰＡＴ：Ｐｒｏｇｒａｍ＿Ａｓｓｏｃｉａｔｉｏｎ＿Ｔａｂｌｅ）と、指定されたプログラムのデータエレメントが記述されたトランスポートストリームパケットを指し示すためのプログラムマップテーブル（ＰＭＴ：Ｐｒｏｇｒａｍ＿Ｍａｐ＿Ｔａｂｌｅ）と、ＥＭＭデータが含まれるトランスポートストリームパケットを指定するための条件付きアクセステーブル（ＣＡＴ：Ｃｏｎｄｉｔｉｏｎａｌ＿Ａｃｃｅｓｓ＿Ｔａｂｌｅ）とから構成されている。エンコーダ／マルチプレクサコントロールユニット９は、プログラムアソシエーションテーブルＰＡＴ、プログラムマップテーブルＰＭＴ及び条件付きアクセステーブルＣＡＴを生成し、これらの生成したテーブルをトランスポートストリームの形態で出力する。以下の説明において、プログラムアソシエーションテーブルＰＡＴを含んだトランスポートストリームパケットをＰＡＴパケットと呼び、プログラムマップテーブルＰＭＴを含んだトランスポートストリームパケットをＰＭＴパケットと呼び、条件付きアクセステーブルＣＡＴを含んだトランスポートストリームパケットをＣＡＴパケットと呼ぶことにする。

また、エンコーダ／マルチプレクサコントロールユニット９は、ＥＰＧシステム４、顧客視聴許可システム３及びエンコーディングシステム７において作成したトランスポートストリームパケットに対して適切なパケット識別子ＰＩＤを設定するために、適切なパケット識別子ＰＩＤを生成顧客視聴許可システム３、ＥＰＧシステム及びエンコーディングシステム７に供給する。

パケット識別子（ＰＩＤ：Ｐａｃｋｅｔ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）は、トランスポートストリームパケットを識別するための識別子である。このパケット識別子ＰＩＤは、トランスポートストリームパケットのペイロード中に蓄積されるデータの種類に応じて決定される１３ビットの固有のデータである。例え

ば、図３に示すように、ペイロード中にプログラムアソシエーションテーブルＰＡＴに関する情報が蓄積されたトランスポートストリームパケットのＰＩＤ値として「０ｘ０００００」が指定され、ペイロード中に条件付きアクセステーブルＣＡＴに関する情報が蓄積されたトランスポートストリームパケットのＰＩＤ値として「０ｘ００００１」が指定されている。また、ペイロード中にビデオデータやオーディオデータ等のエレメンタリーデータやプログラムマップテーブルＰＭＴに関する情報が蓄積されたトランスポートストリームパケットのＰＩＤ値として、「０ｘ００２０」～「０ｘ１ＦＦＥ」の間の何れかのＰＩＤ値が選択される。

また、エンコーダ／マルチプレクサコントロールユニット９は、各トランスポートストリームパケットに対して設定されるＰＩＤを生成する際に、各トランスポートストリームパケットに対して設定したＰＩＤとスクランブル処理に使用するスクランブルキーＫｓとを対応付けたＰＩＤテーブルを生成する。このＰＩＤテーブルは、過去において使用したＰＩＤ値を記憶しておくためのテーブルであって、このエンコーダ／マルチプレクサコントロールユニット９は、このＰＩＤテーブルに記憶されたＰＩＤ値を参照することによって、過去において使用したＰＩＤを認識し、過去のＰＩＤと重複しないような新しいＰＩＤ値を生成することができる。また、このＰＩＤテーブルは、多重化されたトランスポートストリームパケットをスクランブルするかしないかを決定する際に使用されるテーブルである。

例えば、ＰＩＤテーブルは、図４に示すように、生成されたトランスポートストリームパケットに対して設定されたＰＩＤ値と、対応するトランスポートストリームパケットに蓄積されているデータに対して設定されたスクランブルキーとを対応付けたテーブルである。この図４は、ＰＡＴパケットを示すＰＩＤ値は、固定の「０ｘ００００」であって、第１のプログラムに対応するＰＭＴパケットに対して設定されたＰＩＤ値は「０ｘ０１００」であって、第２のプログラムに対応するＰＭＴパケットに対して設定されたＰＩＤ値は「０ｘ０１０１」であって、第１のプログラムのビデオデータのパケットであるＶｉｄｅｏ〔１〕パケッ

ト及びメインオーディオデータのパケットであるＭａｉｎ＿Ａｕｄｉｏ〔１〕パケットをスクランブルするためのスクランブルキーＫｓ１を有したＥＣＭパケットに対して設定されたＰＩＤ値は「０ｘ０３００」であって、第２のプログラムのビデオデータのパケットであるＶｉｄｅｏ〔２〕パケットをスクランブルするためのスクランブルキーＫｓ２を有したＥＣＭパケットに対して設定されたＰＩＤ値は「０ｘ０３０１」であって、第２のプログラムのメインオーディオデータのパケットであるＭａｉｎ＿Ａｕｄｉｏ〔２〕パケットをスクランブルするためのスクランブルキーＫｓ２を有したＥＣＭパケットに対して設定されたＰＩＤ値は「０ｘ０３０２」であって、第２のプログラムのサブオーディオデータのパケットでＳｕｂ＿Ａｕｄｉｏ〔２〕パケットをスクランブルするためのスクランブルキーＫｓ３を含んだＥＣＭパケットに対して設定されたＰＩＤ値は「０ｘ０３０３」であって、第２のプログラムのプライベートデータのパケットであるＰｒｉｖａｔｅ〔２〕パケットをスクランブルするためのスクランブルキーＫｓ４を含んだＥＣＭパケットに対して設定されたＰＩＤ値は「０ｘ０３０４」である。また、第１のプログラムのビテオデータのパケットであるＶｉｄｅｏ〔１〕に対して設定されたＰＩＤ値は「０ｘ０５００」であって、このパケットはスクランブルキーＫｓ１を用いてスクランブルがかけられ、第１のプログラムのメインオーディオデータのパケットであるＭａｉｎ＿Ａｕｄｉｏ〔１〕パケットに対して設定されたＰＩＤ値は「０ｘ０５０１」であって、このパケットはスクランブルキーＫｓ１を用いてスクランブルがかけられ、第２のプログラムのビデオデータのパケットであるＶｉｄｅｏ〔２〕パケットに対して設定されたＰＩＤ値は「０ｘ０５０２」であって、このパケットはスクランブルキーＫｓ２を用いてスクランブルがかけられる。またＣＡＴパケットを示すＰＩＤ値は固定の「０ｘ０００１」であって、ＥＭＭパケットに対して設定されたＰＩＤ値は「０ｘ７００」である。

エンコーディングシステム７は、図５に示されるように、ＭＰＥＧ２規格に基いて供給された複数チャンネルのビデオデータをエンコードするための複数のＭ

ＰＥＧビデオエンコーダ７１１Ｖ～７１９Ｖと、ビデオデータにそれぞれ対応する複数のオーディオデータをＭＰＥＧ２規格に基いて符号化するためのＭＰＥＧオーディオエンコーダ７１１Ａ方７１９Ａと、各ビデオエンコーダ、各オーディオエンコーダからのストリーム及びエンコーダ／マルチプレクサコントロールユニット９から供給されたプライベートデータストリームを多重化するための多重化回路７２１～７２９と、各ビデオ／オーディオエンコーダ７１１～７１９及び多重化回路７２１～７１９をそれぞれ制御するためのエンコーディングコントローラ７０とを有している。この図５に示されるエンコーディングシステムは、９チャンネルのプログラムをエンコードする構成となっているが、９チャンネルに限らず何チャンネルであっても良いことは言うまでもない。

各ビデオエンコーダ７１１Ｖ～７１９Ｖは、ビデオデータをＭＰＥＧ２規格に基いてエンコードすることによって符号化ビットストリームを生成する。続いて、各ビデオエンコーダは、このビットストリームを１ピクチヤ単位で分割すると共にその分割されたビットストリームにヘッダを付加することによつてＰＥＳ（Ｐａｃｋｅｔｉｚｅｄ　Ｅｌｅｍｅｎｔａｒｙ　Ｓｔｒｅａｍ）パケットを生成する。そして、さらに各ビデオエンコーダは、ＰＥＳパケットを１８４バイト単位に分割し、その分割された１８４バイトのビットストリームに４バイトのヘッダを付与することによって、トランスポートストリームパケットを生成する。トランスポートストリームパケットが連続してストリーム状になっているデータのことをトランスポートストリームと呼んでいる。また、トランスポートストリームパケットを生成する際に、エンコーダ／マルチプレクサコントロールユニット９から、各ビデオエンコーダ７１１Ｖ～７１９Ｖに対して、この符号化されたビデオデータを含んだトランスポートストリームパケットを識別するためのパケット識別子（ＰＩＤ）がそれぞれ供給される。

また、各オーディオエンコーダ７１１Ａ～７１９Ａは、メインオーディオデータやサブオーディオデータをＭＰＥＧ２規格に基いてエンコードすることによって符号化されたビットストリームを生成する。ビデオエンコーダと同じように、

各オーディオエンコーダ７１１Ａ～７１９Ａは、このビットストリームからＰＥＳパケットを生成し、このＰＥＳパケットを１８４バイト単位に分割し、４バイトのヘッダを付与することによってオーディオデータを含んだトランスポートストリームパケットを生成する。また、トランスポートストリームパケットを生成する際に、エンコーダ／マルチプレクサコントロールユニット９から、各オーディオエンコーダ７１１Ａ～７１９Ａに対して、この符号化されたオーディオデータを含んだトランスポートストリームパケットを識別するためのパケット識別子（ＰＩＤ）がそれぞれ供給される。

多重化回路７２１～７２９は、符号化ビデオデータを含んだトランスポートストリーム、符号化オーディオデータを含んだトランスポートストリーム及びプライベートデータを含んだトランスポートストリームを多重化して、１つのトランスポートストリームを生成する。具体的には、多重化回路は、符号化ビデオデータを含んだトランスポートストリーム、符号化オーディオデータを含んだトランスポートストリーム及びプライベートデータを含んだトランスポートストリームを、トランスポートストリームパケット単位で切換えることによって、これらのストリームを多重化する。従って、出力されるトランスポートストリーム中には、符号化ビデオデータを含んだトランスポートストリームパケットと、符号化オーディオデータを含んだトランスポートストリームパケットと、プライベートデータを含んだトランスポートストリームパケットが混在している。因みに、プライベートデータはエンコーディングコントローラ７０によつてトランスポートストリームパケット化されてネットワークを介して各多重化回路に供給される。

エンコーディングコントローラ７０は、各ビデオエンコーダ及びオーディオエンコーダに対して、適切な符号化ビットレートを指定する。例えば、エンコーディングコントローラ７０は、スポーツ等の符号化ビット量を多く必要とするプログラムをエンコードするためのエンコーダには、高いビットレートを割当て、ニュース映像などの比較的、符号化時の発生ビット量が少ないと思われるプログラムをエンコードするエンコーダに対しては、低いビットレートを割り当てる。つ

まり、各チャンネルのビデオデータの複雑度（符号化する際にどれだけビット量が発生するかを示す指標として用いられている）を相対的に把握し、複雑度が高いビデオデータのチャンネルから順に高いビットレートを割り当てるようにしている。もちろん、割当てられたビットレートはプログラム固有では無くて、プログラム内のビデオデータの複雑度に応じてその都度変更される。

次に、このトランスポートストリームパケットの構造及びトランスポートストリームパケットのシンタックスについて、図６から図９を参照して詳しく説明する。

トランスポートストリームパケットは、４バイトのヘッダと、各種のデータ及びデータエレメントを格納するための１８４バイトのペーロード部とから構成されている。

トランスポートストリームパケットのヘッダ部は、ｓｙｎｃ＿ｂｙｔｅ、ｔｒａｎｓｐｏｒｔ＿ｅｒｒｏｒ＿ｉｎｄｉｃａｔｏｒ、ｐａｙｌｏａｄ＿ｕｎｉｔ＿ｓｔａｒｔ＿ｉｎｄｉｃａｔｏｒ、ｔｒａｎｓｐｏｒｔ＿ｐｒｉｏｒｉｔｙ＿、ＰＩＤ、ｔｒａｎｓｐｏｒｔ＿ｓｃｒａｍｂｌｉｎｇ＿ｃｏｎｔｒｏｌ、ａｄａｐｔａｔｉｏｎ＿ｆｉｅｌｄ＿ｃｏｎｔｒｏｌ、ｃｏｎｔｉｎｕｉｔｙ＿ｃｏｕｎｔｅｒ、及びａｄａｐｔａｔｉｏｎ＿ｆｉｅｌｄ等の各種フィールドから構成されている。

ｓｙｎｃ＿ｂｙｔｅとは、ビットストリーム中から同期パターンを検出するための固定の８ビットのフィールドである。値は‘０１０００１１１’（ＯＸ４７）の固定値で定義され、このストリーム中のこのビットパターンを検出することによって、同期を検出することができる。

ｔｒａｎｓｐｏｒｔ＿ｅｒｒｏｒ＿ｉｎｄｉｃａｔｏｒは、1ビットのフラグである、「１」に設定されると、少なくとも1ビットの訂正できないビットエラーがトランスポートストリームパケットに存在することを示す。

ｐａｙｌｏａｄ＿ｕｎｉｔ＿ｓｔａｒｔ＿ｉｎｄｉｃａｔｏｒは、1ビットのフラグである。ビデオ／オーディオデータ等のエレメンタリーデータまたはプロ

グラム仕様情報（ＰＳＩ）を伝送するトランスポートストリームパケットに対して規範的な意味を有するデータである。トランスポートストリームパケットのペイロードがエレメンタリーデータを含む場合、ｐａｙｌｏａｄ＿ｕｎｉｔ＿ｓｔａｒｔ＿ｉｎｄｉｃａｔｏｒは、次の意味を有する。ｐａｙｌｏａｄ＿ｕｎｉｔ＿ｓｔａｒｔ＿ｉｎｄｉｃａｔｏｒが「１」の場合には、このトランスポートストリームパケットのペイロードの最初に、エレメンタリーデータが挿入されていることを示し、ｐａｙｌｏａｄ＿ｕｎｉｔ＿ｓｔａｒｔ＿ｉｎｄｉｃａｔｏｒが「０」の場合には、このトランスポートストリームパケットのペイロードの最初に、エレメンタリーデータが挿入されていないことを示す。もし、ｐａｙｌｏａｄ＿ｕｎｉｔ＿ｓｔａｒｔ＿ｉｎｄｉｃａｔｏｒが「１」にセットされると、ただ一つのＰＥＳパケットが任意のトランスポートストリームパケットで開始することを示す。一方、トランスポートストリームパケットのペイロードがＰＳＩデータを含む場合、ｐａｙｌｏａｄ＿ｕｎｉｔ＿ｓｔａｒｔ＿ｉｎｄｉｃａｔｏｒは、次の意味を有する。もし、トランスポートパケットがＰＳＩセクションの第１バイトを伝送する場合、ｐａｙｌｏａｄ＿ｕｎｉｔ＿ｓｔａｒｔ＿ｉｎｄｉｃａｔｏｒは「１」となる。もし、トランスポートストリームパケットがＰＳＩセクションの第１バイトを伝送していない場合、ｐａｙｌｏａｄ＿ｕｎｉｔ＿ｓｔａｒｔ＿ｉｎｄｉｃａｔｏｒは「０」となる。尚、トランスポートストリームパケットがヌルパケットの場合にも、ｐａｙｌｏａｄ＿ｕｎｉｔ＿ｓｔａｒｔ＿ｉｎｄｉｃａｔｏｒは「０」となる。

ｔｒａｎｓｐｏｒｔ＿ｐｒｉｏｒｉｔｙは、トランスポートパケットの優先度を示す１ビットの識別子である。このｔｒａｎｓｐｏｒｔ＿ｐｒｉｏｒｉｔｙが「１」に設定されると、このトランスポートパケットは、同一のパケット識別子ＰＩＤをもつパケットであって、このｔｒａｎｓｐｏｒｔ＿ｐｒｉｏｒｉｔｙが「１」でないパケットより優先度が高いことを示している。例えば、このｔｒａｎｓｐｏｒｔ＿ｐｒｉｏｒｉｔｙのパケット識別子を設定することによって、一つのエレメンタリーストリーム内において任意のパケットに優先度をつけること

ができる。

ｔｒａｎｐｏｒｔ＿ｓｃｒａｍｂｌｉｎｇ＿ｃｏｎｔｒｏｌは、トランスポートストリームパケットペイロードのスクランブリングモードを示す２ビットのデータである。スクランブリングモードとは、ペイロードに格納されたデータがスクランブされているか否か及びそのスクラングルの種類を示すためのモードである。トランスポートストリームパケットヘッダ、およびアダプテーションフィールドは、スクランブルキーＫｓによってスクランブルされてはならないように規格化されている。よって、このｔｒａｎｐｏｒｔ＿ｓｃｒａｍｂｌｉｎｇ＿ｃｏｎｔｒｏｌによって、トランスポートストリームパケットペイロードに格納されたデータがスクランブルされているか否かを判断することができる。

ａｄａｐｔａｔｉｏｎ＿ｆｉｅｌｄ＿ｃｏｎｔｒｏｌは、このトランスポートストリームのパケットヘッダにアダプテーションフィールド及び／又はペイロードがくることを示す２ビットのデータである。具体的には、パケットヘッダにペイロードデータのみが配置される場合には、このａｄａｐｔａｔｉｏｎ＿ｆｉｅｌｄ＿ｃｏｎｔｒｏｌは「０１」となり、パケットヘッダにアダプテーションフィールドのみが配置される場合には、このａｄａｐｔａｔｉｏｎ＿ｆｉｅｌｄ＿ｃｏｎｔｒｏｌは「１０」となり、パケットヘッダにアダプテーションフィールドとペイロードとが配置される場合には、このａｄａｐｔａｔｉｏｎ＿ｆｉｅｌｄ＿ｃｏｎｔｒｏｌは「１１」となる。

ｃｏｎｔｉｎｕｉｔｙ＿ｃｏｕｎｔｅｒは、連続して伝送された同じＰＩＤをもつパケットが、伝送途中で一部欠落又は捨てられか否かを示すためのデータである。具体的には、ｃｏｎｔｉｎｕｉｔｙ＿ｃｏｕｎｔｅｒは、同一のＰＩＤを有する各トランスポートストリームパケットごとに増加する4ビットのフィールドである。但し、このｃｏｎｔｉｎｕｉｔｙ＿ｃｏｕｎｔｅｒがカウントされるときは、パケットヘッダにアダムテーションフィールドが配置されている場合である。

ａｄａｐｔａｔｉｏｎ＿ｆｉｅｌｄは、個別ストリームに関する付加情報やス

タッフィングバイト等をオプションとして挿入するためのフィールドである。このアダプテーションフィールドによって、個別ストリームの動的な状態変化に関するあらゆる情報をデータと一緒に伝送することができる。

adaptation_fieldは、adaptation_field_length、discontitnuity_counter、randam_access_indicator、elementary_stream_priority_indicator、OPCR_flag; splicing_point_flag、splicing_point、transport_private_data_flag、adaptation_filed_extension_flag、program_clock_reference (PCR)、original_program clock_reference (OPCR)、sprice_countdown、transport_private_data_length、private_data、adaptation_filed_extension_length、ltw_flag (legal_time_window flag)、piece_wise_rate_flag、及びSeamless_splice_flag等の各種フィールドから構成されている。

adaptation_field_lengthは、このadaptation_field_lengthの次に続くアダプテーションフィールドのバイト数を示すデータである。adaptation_field_controlが「11」の場合には、adaptation_field_lengthは0から182ビットであって、adaptation_field_controlが「10」の場合には、adaptation_field_lengthは183ビットとなる。尚、トランスポートストリームのペイロードを満たすだけのエレメンタリーストリームが無い場合には、ビットを満たすためのスタッフィング処理が必要となる。

ｄｉｓｃｏｎｔｉｔｎｕｉｔｙ＿ｃｏｕｎｔｅｒは、同じＰＩＤを有する複数のパケットの途中において、システムクロックリファレンス（ＳＣＲ）がリセットされ、システムクロックリファレンスが不連続になっているか否かを示すデータである。もし、システムクロックリファレンスが不連続の場合には、このｄｉｓｃｏｎｔｉｔｎｕｉｔｙ＿ｃｏｕｎｔｅｒは「１」となり、システムクロックリファレンスが連続している場合には、このｄｉｓｃｏｎｔｉｔｎｕｉｔｙ＿ｃｏｕｎｔｅｒは「０」となる。尚、このシステムクロックリファレンスとは、ビデオ及びオーディオのデコードするためのＭＰＥＧデコーダにおいて、デコーダ側のシステムタイムクロックの値をエンコーダ側において意図したタイミングに設定するための参照情報である。

ｒａｎｄａｍ＿ａｃｃｅｓｓ＿ｉｎｄｉｃａｔｏｒは、ビデオのシーケンスヘッダ又はオーディオのフレームの始まりを示すデータである。つまり、このｒａｎｄａｍ＿ａｃｃｅｓｓ＿ｉｎｄｉｃａｔｏｒは、データエレメントのランダムアクセスを行うときに、ビデオ又はオーディオのアクセスポイント（フレームの始まりのこと）であることを示すためのデータである。

ｅｌｅｍｅｎｔａｒｙ＿ｓｔｒｅａｍ＿ｐｒｉｏｒｉｔｙ＿ｉｎｄｉｃａｔｏｒは、同一のＰＩＤを有するパケットにおいて、このトランスポートストリームパケットのペイロード中で伝送されるエレメンタリーストリームデータの優先度を示すデータである。例えば、エレメンタリーストリームのビデオデータが、そのビデオデータがイントラ符号化されている場合に、ｅｌｅｍｅｎｔａｒｙ＿ｓｔｒｅａｍ＿ｐｒｉｏｒｉｔｙ＿ｉｎｄｉｃａｔｏｒが「１」にセットされる。それに対して、インター符号化されているビデオデータを含んだトランスポートストリームのｅｌｅｍｅｎｔａｒｙ＿ｓｔｒｅａｍ＿ｐｒｉｏｒｉｔｙ＿ｉｎｄｉｃａｔｏｒは、「０」にセットされる。

ＰＣＲ＿ｆｌａｇは、アダプテーションフィールド内にＰＣＲ（ｐｒｏｇｒａｍ＿ｃｌｏｃｋ＿ｒｅｆｅｒｅｎｃｅデータが存在するか否かを示すデータでる。アダプテーションフィールド内にＰＣＲデータが存在する場合には、Ｐ

ＣＲ＿ｆｌａｇが「１」にセットされ、ＰＣＲデータが存在しない場合には、ＰＣＲ＿ｆｌａｇが「０」にセットされる。尚、このＰＣＲデータとは、受信機側のデコーダにおいて、伝送されたデータをデコードするデコード処理のタイミングを得るために使用されるデータである。

ＯＰＣＲ＿ｆｌａｇは、アダプテーションフィールド内にＯＰＣＲ（ｏｒｉｇｉｎａｌ＿ｐｒｏｇｒａｍ＿ｃｌｏｃｋ＿ｒｅｆｅｒｅｎｃｅデータが存在するか否かを示すデータでる。アダプテーションフィールド内にＯＰＣＲデータが存在する場合には、ＯＰＣＲ＿ｆｌａｇが「１」にセットされ、ＯＰＣＲデータが存在しない場合には、ＯＰＣＲ＿ｆｌａｇが「０」にセットされる。このＯＰＣＲデータとは、スプラインシング処理等によって、複数のオリジナルトランスポートストリームから１つのトランスポートストリームを再構築したときのに使用されるデータであって、あるオリジナルトランスポートストリームのＰＣＲデータを表わすデータである。

ｓｐｌｉｃｉｎｇ＿ｐｏｉｎｔ＿ｆｌａｇは、トランスポートレベルでの編集ポイント（スプライスポイント）を示すためのｓｐｌｉｃｅ＿ｃｏｕｎｔ－ｄｏｗｎがアダプテーションフィールド内に存在するか否かを示すデータである。アダプテーションフィールド内に＾ｐｌｉｃｅ＿ｃｏｕｎｔｄｏｗｎが存在する場合には、このｓｐｌｉｃｉｎｇ＿ｐｏｉｎｔ＿ｆｌａｇは「１」であって、アダプテーションフィールド内にｐｌｉｃｅ＿ｃｏｕｎｔｄｏｗｎが存在する場合には、このｓｐｌｉｃｉｎｇ＿ｐｏｉｎｔ＿ｆｌａｇは「０」である。

ｔｒａｎｓｐｏｒｔ＿ｐｒｉｖａｔｅ＿ｄａｔａ＿ｆｌａｇは、アダプテーションフィールド内に、任意のユーザデータを記述するためのプライベートが存在するか否かを示すためのデータである。アダプテーションフィールド内にプライベートが存在する場合には、このｔｒａｎｓｐｏｒｔ＿ｐｒｉｖａｔｅ＿ｄａｔａ＿ｆｌａｇ「１」にセットされ、アダプテーションフィールド内にプライベートが存在しない場合には、このｔｒａｎｓｐｏｒｔ＿ｐｒｉｖａｔｅ＿ｄａｔａ＿ｆｌａｇは「０」にセットされる。

adaptation_field_extension_flagは、アダプテーションフィールド内に、拡張フィールド存在するか否かを示すためのデータである。アダプテーションフィールド内に拡張フィールドが存在する場合には、このadaptation_field_extension_flagは「1」にセットされ、アダプテーションフィールド内に拡張フィールドが存在しない場合には、このadaptation_field_extension_flagは「0」にセットされる。

program_clock_reference（PCR）は、送信側とクロックの位相に対して受信機側のクロックの位相を同期させるときに参照する基準クロックである。このPCRデータには、トランスポートパケットが生成された時間が格納されている。このPCRは、33ビットのprogram_clock_reference_baseと9ビットのprogram_clock_reference_extensionとの42ビットから構成されるデータである。program_clock_reference_extensionによって0～299までのシステムクロックをカウントし、299から0にリセットされる際のキャリーによって、program_clock_reference_baseに1ビットを加算することによって、24時間をカウントすることができる。

original_program_clock_reference（IOPCR）は、あるトランスポートストリームから単一プログラムのトランスポートストリームを再構成するときに使用されるデータである。単一プログラムドランスポートストリームが完全に再構成された場合、このoriginal_program_clock_referenceはprogram_clock_referenceにコピーされる。

splice_countdownは、同一PIDのトランスポートストリームパケットにおいて、トランスポートストリームパケットレベルで編集可能（スプライシング処理可能）なポイントまでのパケットの数を示すデータである。従

って、編集可能なスプライシングポイントのトランスポートストリームパケットでは、ｓｐｌｉｃｅ＿ｃｏｕｎｔｄｏｗｎは「０」である。ｓｐｌｉｃｅ＿ｃｏｕｎｔｄｏｗｎが「０」になるトランスポートパケットで、トランスポートストリームパケットペイロードの最終バイトは、符号化されたピクチャの最後のバイトとすることによって、スプライシング処理が可能となる。

このスプライシング処理とは、トランスポートレベルで行われる２つの異なるエレメンタリーストリームを連結し、１つの新しいトランスポートストリームを生成する処理のことである。そして、スプライシング処理として、復号の不連続性を発生しないシームレススプライスと、復号の不連続性を引き起こすノンシームレススプライスとに分けることができる。符号の不連続性を発生しないとは、新しく後ろにつなげられたストリームのアクセスユニットの復号時間と、スプライス前の古いストリームのアクセスユニットの復号時間と間の矛盾が無いことを示し、符号の不連続性を発生するとは、新しく後ろにつなげられたストリームのアクセスユニットの復号時間に対して、スプライス前の古いストリームのアクセスユニットの復号時間の矛盾が生じることを示している。

ｔｒａｎｓｐｏｒｔ＿ｐｒｉｖａｔｅ＿ｄａｔａ＿ｌｅｎｇｔｈは、アダプテーションフィールドにおけるプライデートデータのバイト数を示すデータである。

ｐｒｉｖａｔｅ＿ｄａｔａは、規格では特に規定されておらず、アダプテーションフィールドにおいて任意のユーザデータを記述することができるフィールドである。

ａｄａｐｔａｔｉｏｎ＿ｆｉｅｌｄ＿ｅｘｔｅｎｓｉｏｎ＿ｌｅｎｇｔｈは、アダプテーションフィールドにおけるアダプテーションフィールドエクステンションのデータ長を示すデータである。

ｌｔｗ＿ｆｌａｇ（ｌｅｇａｌ＿ｔｉｍｅ＿ｗｉｎｄｏｗ＿ｆｌａｇ）は、アダプテーションフィールドにおいて表示ウインドウのオフセット値を示すｌｔｗ＿ｏｆｆｓｅｔが存在するか否かを示すデータでる。

ｐｉｅｃｅｗｉｓｅ＿ｒａｔｅ＿ｆｌａｇは、アダプテーションフィールドにおいてｐｉｅｃｅｗｉｓｅ＿ｒａｔｅが存在するか否かを示すデータでる。

ｓｅａｍｌｅｓｓ＿ｓｐｌｉｃｅ＿ｆｌａｇは、スプライシングポイントが、通常のスプライシングポイントか、シームレススプライシングポイントであるかを示すデータである。このｓｅａｍｌｅｓｓ＿ｓｐｌｉｃｅ＿ｆｌａｇが「０」の時は、スプライシングポイントが通常のスプライシングポイントであることを示し、このｓｅａｍｌｅｓｓ＿ｓｐｌｉｃｅ＿ｆｌａｇが「１」の時は、スプライシングポイントがシームレススプイシングポイントであることを示している。通常のスプライシングポイントとは、スプライシングポイントがＰＥＳパケットの区切りに存在する場合であって、このスプライシングポイントの直前のスプライシングパケットがアクセスユニットで終了し、次の同じＰＩＤを有するトランスポートパケットがＰＥＳパケットのヘッダで開始している場合である。これに対して、シームレススプライシングポイントとは、ＰＥＳパケットの途中にスプライシングポイントがある場合であって、新しく後ろにつなげられたストリームのアクセスユニットの復号時間と、スプライス前の古いストリームのアクセスユニットの復号時間との間に矛盾が無いようにするために、古いストリームの特性の一部を、新しいストリームの特性として使う場合である。

次に、図１０を参照してマルチプレクサシステム８について詳細に説明する。このマルチプレクサシステム８は、ＰＡＴパケット、ＰＭＴパケット、ＣＡＴパケット、符号化されたエレメンタリデータを含んだトランスポートストリームパケット、ＥＰＧパケット、ＥＣＭパケット、及びＥＭＭ．ケットを多重化し、１つのトランスポートストリームを生成するためのシステムである。

具体的には、このマルチプレクサシステム８は、このマルチプレクサシステム８内の全ての回路を管理するマルチプレクサコントローラ８１と、顧客視聴許可システム３から供給されたＥＣＭパケットを暗号化するための暗号化ブロック８２と、エンコーダ／マルチプレクサシステム９からプログラム仕様情報ＰＳＩとして供給されたＰＡＴパケット、ＰＭＴパケット及びＣＡＴパケットをそれぞれ

バッファリングするためのＦＩＦＯバッファ８４１～８４３、複数のプログラムを含んだトランスポートストリームパケットをそれぞれバッファリングするためのＦＩＦＯバッファ８５１～８５９、ＥＣＭパケット、ＥＭＭパケット及びＥＰＧパケットをそれぞれバッファリングするためのＦＩＦＯバッファ８６１～８６３、各ＦＩＦＯバッファのリード／ライトを制御すると共に、各ＦＩＦＯバッファの空き容量を監視するＦＩＦＯコントローラ８３と、各ＦＩＦＯバッファから出力されたトランスポートストリームパケットを多重化して多重化されたトランスポートストリームを生成する多重化回路８７と、多重化されたトランスポートストリームパケットに含まれるデータエレメントにスクランブルを施すスクランブルブロック８８とを備えている。

マルチプレクサコントローラ８１は、エンコーダ／マルチプレクサコントロールユニット９からＥＰＧパケット、ＥＭＭ'パケット、ＥＣＭパケット（ＥＣＭ１～ＥＣＭ１９）、ＰＡＴパケット、ＰＭＴパケット及びＣＡＴパケットを受取り、各パケットを適切な回路に供給する。また、マルチプレクサコントローラ８１は、エンコーダ／マルチプレクサコントロールユニット９からＰＩＤテーブルを受取り、このＰＩＤテーブルをスクランブルブロック８８に供給する。

暗号化ブロック８２は、エンコーダ／マルチプレクサコントロールユニット９及びマルチプレクサコントローラ８１を介して顧客視聴許可システム３から供給された複数のＥＣＭパケットに含まれるスクランブルキーＫｓを暗号化（Ｅｎｃｒｙｐｔ）するためのブロックである。暗号化ブロック８２は、顧客視聴許可システム３からダウンロードされたワークキーテーブルを暗号化処理の前に予め記憶しておくためのＲＡＭ８２１と、ワークキーＫｗに基いてＥＣＭに含まれるスクランブルキーＫｓを暗号化する暗号化回路（Ｅｎｃｒｙｐｔｅｒ）８２２とを有している。

次に、この暗号化ブロック８２における暗号化処理の動作を、第１のプログラムを構成するエレメンタリーデータをスクランブルするためのスクランブルキーＫｓ１を暗号化する場合を例にあげて説明する。まず、ＥＣＭパケットＥＣＭ１

に含まれるワークキー番号Kw_Noが、ＲＡＭ８２１に供給される。ＲＡＭ８２１には、顧客視聴許可システムからダウンロードされたワークキー番号Ｋｗ＿Ｎｏとワークキー Ｋｗとを対応付けたワークキーテーブルが記憶されている。従って、ＲＡＭ８２１にはＥＣＭ１に含まれていたワークキー番号Kw_Noが供給されるので、供給されたワークキー番号Ｋｗ＿Ｎｏに対応したワークキーＫｗがこのＲＡＭ８２１から出力される。暗号化回路８２２は、スクランブルキーＫｓ１を含んだＥＣＭパケットを受け取ると共に、ワークキーＫｗをＲＡＭ８２１から受け取る。この暗号化回路８２２は、このワークキーＫｗを使用して、ソースＥＣＭに含まれているスクランブルキーＫｓ１を暗号化し、暗号化されたスクランブルキーＫｓ１’を生成する。暗号化回路８２２は、ソースＥＣＭの暗号化されていないスクランブルキーＫｓの代わりに暗号化されたスクランブルキーＫｓ’を蓄積し、この暗号化スクランブルキーＫｓ１’を含んだトランスポートストリームパケットを、暗号化ＥＣＭパケットとして出力する。尚、この暗号化アルゴリズムは、顧客視聴許可システム３において、ＥＭＭデータに含まれるワークキーＫｗを暗号化したときの暗号化アルゴリズムＣＲＹＳＰと同じアルゴリズムである。

一方、この暗号化ブロック８２は、ＥＣＭデータとして供給されたスクランブルキーＫｓ１を、スクランブルブロック８８に供給する。尚、このスクランブルブロック８８に供給されるスクランブルキーＫｓ１は、ワークキーＫｗによって暗号化されていないキーである。

第１のＥＣＭパケットＥＣＭに蓄積されているスクランブルキーＫｓ１を暗号化する例について説明したが、他のスクランブルキーＫｓ２～Ｋｓ１９を暗号化する処理も全く同じである。よって、暗号化ブロック８２からは、暗号化ＥＣＭパケットＥＣＭ１’～ＥＣＭ１９’が出力されてＦＩＦＯバッファ８６１に供給されると共に、暗号化ブロック８２からは、暗号化されていないスクランブルキーＫｓ１～Ｋｓ１９が出力されてスクランブルブロック８８に供給される。

多重化回路８７は、ＦＩＦＯ８４１～８４３にバッファリングされたＰＡＴパ

ケット、ＰＭＴパケット又はＣＡＴパケット、ＦＩＦＯ８５１～８５９にバッファリングされた複数のプログラムＰｒｏｇｒａｍ１～Ｐｒｏｇｒａｍ９をそれぞれ含んだ各トランスポートストリームパケット、ＦＩＦＯ８６１～８６３にバッファリングされたＥＣＭパケット、ＥＭＭパケット又はＥＰＧパケットのいずれかを、各ＦＩＦＯのデータ量に応じて選択しながらスクランブルブロック８８に供給する。このとき、ＦＩＦＯコントローラ８３は各ＦＩＦＯに入力されるパケットデータの入力レートを監視しており、各ＦＩＦＯごとの入力レートの総和が所定の出力レートを越えているとき、この過入力レートの状態をマルチプレクサコントローラ８１に供給する。この結果、マルチプレクサコントローラ８１は、多重化回路８７によつて選択される選択対象としての各ＦＩＦＯのうち、ＥＭＭパケットをバッファリングするＦＩＦＯ８６２を選択対象外に除外し、残りのＦＩＦＯを選択対象として切り換えながら、その切り換えられたＦＩＦＯのパケットデータをスクランブルブロック８８に供給する。この結果、多重化回路８７は選択すべきＦＩＦＯの数が少なくなることにより、選択対象であるＦＩＦＯの選択回数が増加し、これにより過入力レート状態に対応して各ＦＩＦＯのデータ出力レートを増加させることができる。

そして、各ＦＩＦＯごとの入力レートの総和が所定の出力レートを下回ったとき、マルチプレクサコントローラ８１はＦＩＦＯ８６２を多重化回路８７の選択対象に復帰させることにより、ＦＩＦＯ８６２にバッファリングされているＥＭＭパケットをスクランブルブロック８８に供給する。この場合、ＦＩＦＯ８６２にバッファリングされている視聴者の契約内容を表すＥＭＭデータは、そのデータ内容が頻繁に変更されることがなく、多重化回路８７による選択対象から一時的に除外されても、実用上不都合を生じさせることはない。

また、各ＦＩＦＯごとの入力レートの総和がさらに増加して、１つのＦＩＦＯ８６２を多重化回路８７の選択対象外に除外するだけでは過入力レート状態に対応しきれなくなると、マルチプレクサコントローラ８１は、ＥＭＭデータをバッファリングしているＦＩＦＯ８６２に加えて、ＥＰＧデータをバッファリングし

ているＦＩＦＯ８６３を選択対象外に除外する。これにより、多重化回路８７によつて選択されるＦＩＦＯの数がさらに少なくなり、選択対象であるＦＩＦＯの選択回数がさらに増加し、これによりこのときの過入力レート状態に対応して各ＦＩＦＯのデータ出力レートをさらに増加することができる。この場合、ＦＩＦＯ８６３にバッファリングされている番組ガイド情報であるＥＰＧデータは、そのデータ内容が頻繁に変更されることがなく、多重化回路８７による選択対象から一時的に除外されても、実用上不都合を生じさせることはない。

スクランブルブロック８８は、ＰＩＤ検出回路８８１と、スクランブル回路８８２とを有している。ＰＩＤ検出回路８８１は、多重化回路８７から出力されたトランスポートストリームパケットを受け取ると共に、エンコーダ／マルチプレクサコントロールユニット９からマルチプレクサコントローラ８１を介してＰＩＤテーブル（図４）を受け取る。このＰＩＤテーブルには、トランスポートストリームを生成する際に使用したＰＩＤ値とスクランブルキーとが対応付けられて記憶されているので、ＰＩＤ検出回路８８１はＰＩＤテーブルに登録されたＰＩＤ値を参照することによって、使用するスクランブルキーＫｓを検索し、その検索されたスクランブルキーＫｓをスクランブル回路８８２に供給する。スクランブル回路８８２は、ＰＩＤ検出回路８８１から供給されたスクランブルキーＫｓを用いて、このスクランブルキーＫｓに対応付けられたプログラムデータを含むトランスポートストリームパケットにスクランブルをかけ、変調回路１０（図１）に出力する。

次にプログラム仕様情報について説明する。

プログラム仕様情報（ＰＳＩ：Ｐｒｏｇｒａｍ＿Ｓｐｅｃｉｆｉｃ＿Ｉｎｆｏｒｍａｔｉｏｎ）とは、複数プログラム及びデータが多重化されたトランスポートストリームパケットのどのパケットにどのようなデータが含まれているのかを示す情報である。従って、復号器はこのプログラム仕様情報を参照することによって、所望のデータをデコードすることができる。

このプログラム仕様情報は、図１１に示す４つのテーブル構造に分類すること

ができる。プログラムアソシエーションテーブル（ＰＡＴ：Ｐｒｏｇｒａｍ＿Ａｓｓｏｃｉａｔｉｏｎ＿Ｔａｂｌｅ）は、指定されたプログラム番号とそのプログラム番号に対応するプログラムマップテーブル（ＰＭＴ）のＰＩＤを指し示すためのテーブルである。プログラムマップテーブル（ＰＭＴ：Ｐｒｏｇｒａｍ＿Ｍａｐ＿Ｔａｂｌｅ）は、指定されたプログラムのエレメントが記述されたパケットのＰＩＤを指し示すためのテーブルである。網情報テーブル（ＮＩＴ：Ｎｅｔｗｏｒｋ＿Ｉｎｆｏｒｍａｔｉｏｎ＿Ｔａｂｌｅ）は、ネットワークに関するパタメータを伝送する際に仕様する情報であるが、規格では特に規定されていないプライベートなテーブルである。条件付きアクセステーブル（ＣＡＴ：Ｃｏｎｄｉｔｉｏｎａｌ＿Ａｃｃｅｓｓ＿Ｔａｂｌｅ）は、ＥＭＭパケットに固有のＰＩＤを割り当てるためのテーブルである。以下に、プログラムアソシエーションテーブル、プログラムマップテーブル及び条件付きアクセステーブルについて詳細に説明する。

まず、図１２及び図１３を参照して、プログラムアソシエーションテーブルに関して説明する。

プログラムアソシェーションテーブルＰＡＴは、伝送される各プログラムとそのプログラムの内容を指定しているトランスポートストリームパケットのＰＩＤを指定するためのテーブルである。具体的には、このプログラムアソシェーションテーブルＰＡＴは、ｔａｂｌｅ＿ｉｄとｓｅｃｔｉｏｎ＿ｓｙｎｔａｘ＿ｉｎｄｉｃａｔｏｒと、ｓｅｃｔｉｏｎ＿ｌｅｎｇｔｈと、ｔｒａｎｓｐｏｒｔ＿ｓｔｒｅａｍ＿ｉｄと、ｖｅｒｓｉｏｎ＿ｎｕｍｂｅｒと、ｃｕｒｒｅｎｔ＿ｎｅｘｔ＿ｉｎｄｉｃａｔｏｒと、ｓｅｃｔｉｏｎ＿ｎｕｍｂｅｒと、ｌａｓｔ＿ｓｅｃｔｉｏｎ＿ｎｕｍｂｅｒと、ｐｒｏｇｒａｍ＿ｎｕｍｂｅｒと、ｎｅｔｗｏｒｋ＿ＰＩＤと、ｐｒｏｇｒａｍ＿ｍａｐ＿ＰＩＤとから構成されている。

ｔａｂｌｅ＿ｉｄは、図１４に示すように、各テーブルに対して割当てられた固有の識別番号である。プログラムアソシエーションテーブルＰＡＴのｔａｂｌｅ＿ｉｄは「０ｘ００」であって、条件付きアクセステーブルＣＡＴの

ｔａｂｌｅ＿ｉｄは「０ｘ０１」であって、プログラムマップテーブルＰＭＴのｔａｂｌｅ＿ｉｄは「０ｘ０２」である。

ｓｅｃｔｉｏｎ＿ｓｙｎｔａｘ＿ｉｎｄｉｃａｔｏｒは、「１」に固定された定数である。

ｓｅｃｔｉｏｎ＿ｌｅｎｇｔｈは、このｓｅｃｔｉｏｎ＿ｌｅｎｇｔｈの後のビットからＣＲＣセクションの最後のバイトまでのバイト数を示すフィールドである。

ｔｒａｎｓｐｏｒｔ＿ｓｔｒｄｅａｍ＿ｉｄは、このトランスポートストリームとネットワーク中に多重化されている他のトランスポートストリームとを識別するための識別データである。

ｖｅｒｓｉｏｎ＿ｎｕｍｂｅｒは、プログラムアソシエーションテーブル（ＰＡＴ）のバージョン番号を示すデータである。このバージョン番号とは、プログラムアソシエーションテーブルの設定が変更されたときに、つまり、トランスポートストリームの特性が変化する場合に１づつインクリメントされる０から３１までの整数である。受信機側の復号器においては、このｖｅｒｓｉｏｎ＿ｎｕｍｂｅｒを参照し、最も新しいバーションのセクションのみを有効と判断するようにしている。

ｃｕｒｒｅｎｔ＿ｎｅｘｔ＿ｉｎｄｉｃａｔｏｒは、伝送されているプログラムアソシエーションテーブルが現在使用可能であるか否かを示すデータである。

ｓｅｃｔｉｏｎ＿ｎｕｍｂｅｒは、このプログラムアソシエーションテーブルセクションの番号を示すデータである。例えば、プログラムアソシエーションテーブルに含まれるｐｒｏｇｒａｍ＿ａｓｓｏｃｉａｔｉｏｎ＿ｓｅｃｔｉｏｎ（）のｓｅｃｔｉｏｎ＿ｎｕｍｂｅｒは、最初のセクションであることを示すために、「０ｘ００」に設定される。

ｌａｓｔ＿ｓｅｃｔｉｏｎ＿ｎｕｍｂｅｒは、このプログラムアソシエーションテーブルによって規定されている全てのセクションの中で最後のセクションのセクション番号を示すデータである。従って、このｌａｓｔ＿ｓｅｃｔｉｏｎ＿

ｎｕｍｂｅｒによってプログラムアソシエーションテーブルによって規定されているセクション数を把握することができる。

ｐｒｏｇｒａｍ＿ｎｕｍｂｅｒは、多重化される複数のプログラムに対して付与された固有の番号である。例えば、本発明のデータ伝送装置においては、多重化される９個のプログラム対して、１から９のプログラム番号が割当てられている。このｐｒｏｇｒａｍ＿ｎｕｍｂｅｒはユーザによって任意に定義することのできるデータである。但し、このｐｒｏｇｒａｍ＿ｎｕｍｂｅｒが０にセットさせているときは、このｐｒｏｇｒａｍ＿ｎｕｍｂｅｒは、ストリーム中にネットワークインフォメーションテーブる（ＮＩＴ）が存在していることを示す。

ｎｅｔｗｏｒｋ＿ＰＩＤは、ストリーム中のネットワークインフォメーションテーブル（ＮＩＴ）が記述されているＰＩＤを指し示すためのデータである。このネットワークインフォメーションテーブル（ＮＩＴ）はユーザによって自由に設定することのできるテーブルであって、今回の装置においては使用されていない。

ｐｒｏｇｒａｍ＿ｍａｐ＿ｐｉｄは、ｐｒｏｇｒａｍ＿ｎｕｍｂｅｒで規定したプログラムに適用されるプログラムマップテーブルを有するトランスポートストリームパケットのＰＩＤを示すデータである。例えば、あるプログラムが１つのビデオデータと４つのオーディオデータから構成されている場合には、このプログラムアソシエーションテーブル内に、そのあるプログラムのビデオデータを有するトランスポートストリームパケットを指定する１つのＰＩＤと、そのあるプログラムのオーディオデータを有するトランスポートストリームパケットを指定する４つのＰＩＤとが記述されている。

次に、図１５及び図１６を参照してプログラムマップテーブル（ＰＭＴ）に関して説明する。

プログラムマップテーブルは、プログラム番号とそれらを構成するデータエレメント間のマッピングを与える。つまり、プログラムマップテーブルは、各プログラム番号毎に、そのプログラムを構成するビデオデータ、オーディオ及び付加

データ等のエレメントが伝送されるトランスポートストリームパケットのＰＩＤを指定するためのセクションである。具体的には、このプログラムマップテーブルは、ｔａｂｌｅ＿ｉｄと、ｓｅｃｔｉｏｎ＿ｓｙｎｔａｘ＿ｉｎｄｉｃａｔｏｒ と、ｓｅｃｔｉｏｎ＿ｌｅｎｇｔｈと、ｐｒｏｇｒａｍ＿ｎｕｍｂｅｒと、ｖｅｒｓｉｏｎ＿ｎｕｍｂｅｒと、ｃｕｒｒｅｎｔ＿ｎｅｘｔ＿ｉｎｄｉｃａｔｏｒと、ｓｅｃｔｉｏｎ＿ｎｕｍｂｅｒと、ｌａｓｔ＿ｓｅｃｔｉｏｎ＿ｎｕｍｂｅｒと、ＰＣＲ＿ＰＩＤと、ｐｒｏｇｒａｍ＿ｉｎｆｏ＿ｌｅｎｇｔｈと、ｄｅｓｃｒｉｐｔｏｒ（）と、ｓｔｒｅａｍ＿ｔｙｐｅと、ｅｌｅｍｅｎｔａｒｙ＿ＰＩＤと、ＥＳ＿ｉｎｆｏ＿ｌｅｎｇｔｈと、ｄｅｓｃｒｉｐｔｏｒ（）とから構成される。

ｔａｂｌｅ＿ｉｄは、各テーブルを識別するために付与された固有の識別番号であって、プログラムマップテーブルのｔａｂｌｅ＿ｉｄは「０ｘ０２」である。

ｓｅｃｔｉｏｎ＿ｓｙｎｔａｘ＿ｉｎｄｉｃａｔｏｒは、「１」に固定された定数である。

ｓｅｃｔｉｏｎ＿ｌｅｎｇｔｈは、このｓｅｃｔｉｏｎ＿ｌｅｎｇｔｈの後のビットからＣＲＣセクションの最後のバイトまでのバイト数を示すフィールドである。

ｐｒｏｇｒａｍ＿ｎｕｍｂｅｒは、多重化される複数のプログラムに対して付与された固有の番号である。例えば、本発明のデータ伝送装置においては、多重化される９個のプログラム対して、１から９のプログラム番号が割当てられている。

ｖｅｒｓｉｏｎ＿ｎｕｍｂｅｒは、プログラムマップテーブルを構成するためのプログラムマップセクションのバージョン番号を示すデータである。このバージョン番号は、プログラムマップセクションにおいて伝送されるデータが変更された場合に、バージョン番号がアップされる。

ｃｕｒｒｅｎｔ＿ｎｅｘｔ＿ｉｎｄｉｃａｔｏｒは、伝送されているプログラ

ムアソシエーションテーブルが現在使用可能であるか否かを示すデータである。プログラムアソシエーションテーブルが現在使用可能であれば、このｃｕｒｒｅｎｔ＿ｎｅｘｔ＿ｉｎｄｉｃａｔｏｒは「１」にセットされ、プログラムアソシエーションテーブルが現在使用可能でないならば、このｃｕｒｒｅｎｔ＿ｎｅｘｔ＿ｉｎｄｉｃａｔｏｒは「０」にセットされる。

ｓｅｃｔｉｏｎ＿ｎｕｍｂｅｒは、このプログラムマップテーブルに含まれているセクションの番号を示すデータであって、常に「０ｘ００」にセットされている。なぜなら、このプログラムマップテーブルを構成するためにはプログラムマップセクションの１つしか存在しないからである。

ｌａｓｔ＿ｓｅｃｔｉｏｎ＿ｎｕｍｂｅｒは、このプログラムマップテーブルによって規定されているセクションの中で最後のセクションのセクション番号を示すデータである。従って、プログラムマップテーブルを構成するためのプログラムマップセクションにおいては、このｌａｓｔ＿ｓｅｃｔｉｏｎ＿ｎｕｍｂｅｒは常に「０ｘ００」にセットされている。

ＰＣＲ＿ＰＩＤは、ｐｒｏｇｒａｍ＿ｎｕｍｂｅｒで規定されるプログラムに対して有効であるＰＣＲデータを含んでいるトランスポートパケットのＰＩＤを示すデータである。

ｐｒｏｇｒａｍ＿ｉｎｆｏ＿ｌｅｎｇｔｈは、このフィールドｐｒｏｇｒａｍ＿ｉｎｆｏ＿ｌｅｎｇｔｈの次に記述されているｄｅｓｃｒｉｐｔｏｒ（）のバイト数を規定するためのデータである。

ｄｅｓｃｒｉｐｔｏｒ（）は、プログラム及びプログラムエレメントの定義を拡張するために使用されるデータ構造である。例えば、ビデオエレメンタリーストリームの符号化パラメータを識別する基本的な情報を記述するためのｖｉｄｅｏ＿ｓｔｒｅａｍ＿ｄｅｓｃｒｉｐｔｏｒ（）や、オーディオエレメンタリーストリームの符号化バージョンを識別する基本的な情報を記述するためのＡｕｄｉｏ＿＿ｓｔｒｅａｍ＿ｄｅｓｃｒｉｐｔｏｒ（）や、複数のストリーム中に多重されている階層符号化されたビデオ及びオーディオを含むプログラムエ

レメント識別するための情報を記述するｈｉｅｒａｒｃｈｙ＿ｄｅｓｃｒｉｐ－ｔｏｒ（）や、プライベートデータを固有且つ明確に識別するための情報を記述するｒｅ－ｓｉｓｔｒａｔｉｏｎ＿ｄｅｓｃｒｉｐｔｏｒ（）や、相互に関連するエレメンタリーストリーム中に存在するアライメントの種類を記述するｄａｔａ＿ｓｔｒｅａｍ＿ａｌｉｇｎｍｅｎｔ＿ｄｅｓｃｒｉｐｔｏｒ（）や、伝送されたビデオデータの表示ウインドウの背景に表示されるバックグラウンドウインドウを指定するための情報を記述するｔａｒｇｅｔ＿ｂａｃｋｇｒｏｕｎｄ＿ｄｅｓｃｒｉｐｔｏｒや、伝送されたビデオデータの表示ウインドウの表示位置を指定するための情報を記述するｖｉｄｅｏ＿ｗｉｎｄｏｗ＿ｄｅｓｃｒｉｐ－ｔｏｒや、受信契約情報ＥＭＭや番組解読情報ＥＣＭ等のデータを記述するためのＣＡ＿ｄｅｓｃｒｉｐｔｏｒ（）や、言語及び関連するプログラムエレメントが使用する言語を識別するための情報が記述されるｌａｎｇｕａｇｅ＿ｄｅ－ｓｃｒｉｐｔｏｒ（）や、タイムスタンプの生成に使用されたシステムクロックに関する情報を伝送するためのｓｙｓ－ｔｅｍ＿ｃｌｏｃｋ＿ｄｅｓｃｒｉｐ－ｔｏｒ（）や、ｖｉｄｅｏ＿ｂｕｆｆｅｒ＿ｖｅｒｉｆｉｅｒを含むＳＴＤ（ｓｙｓｔｅｍ＿ｔａｒｇｅｔ＿ｄｅｃｏｄｅｒ）多重バッファにおけるデータ占有量のアンダーフロー及びオーバーフローの限界レベルを与えるためのデータを記述するｍｕｌｔｉｐｌｅｘ＿ｂｕｆ－ｆｅｒ＿ｕｔｉｌｉｚａｔｉｏｎ＿ｄｅｓｃｒｉｐｔｏｒ（）や、オーディオ／ビジュアル作品の著作権を保護するために、それさを識別を可能とするための情報を記述するｃｏｐｙｒｉｇｈｔ＿ｄｅｓｃｒｉｐｔｏｒ（）や、伝送されるデータエレメントの最大ビットレートを規定するための情報を記述するｍａｘｉ－ｍｕｍ＿ｂｉｔｒａｔｅ＿ｄｅｓｃｒｉｐｔｏｒ（）や、プライベータの伝送を規定するためのｐｒｉ－ｖａｔｅ＿ｄａｔａ＿ｉｎｄｉｃａｔｏｒ＿ｄｅｓｃｒｉｐｔｏｒ（）や、スムージングバッファのサイズ及びそのバッファから出力されるリークレートに関する情報を記述するためのｓｍｏｏｔｈｉｎｇ＿ｂｕｆｆｅｒ＿ｄｅｓｃｒｉｐ－ｔｏｒ（）や、ＳＴＤバッファのリーク値を規定するためのＳＴＤ＿

ｄｅｓｃｒｉｐｔｏｒ（）や、符号化タイプに関する情報を記述するためのｉｂｐ＿ｄｅｓｃｒｉｐｔｏｒ（）などの様々なディスクリプタから構成されている。

本発明のデータ伝送装置においては、このプログラムマップテーブルの中でこのｄｅｓｃｒｉｐｔｏｒ（）が使用される場合には、このｄｅｓｃｒｉｐｔｏｒ（）は、番組解読情報ＥＣＭを含むトランスポートストリームパケットのＰＩＤを指定するための情報を記述するために使用されている。

ｓｔｒｅａｍ＿ｔｙｐｅは、次のｅｌｅｍｅｎｔａｒｙ＿ＰＩＤによって規定されるＰＩＤを有するパケットに含まれるプログラムエレメントのタイプを規定するためのデータである。例えば、このｓｔｒｅａｍ＿ｔｙｐｅは、パケットに含まれるプログラムエレメントが、ＩＳＯ／ＩＥＣ１１１７２規格のビデオデータであれば「０ｘ０１」という値に設定され、ＩＳＯ／ＩＥＣ１３８１８－２規格のビデオデータであれば、「０ｘ０２」という値に設定され、ＩＳＯ／ＩＥＣ１１１７２規格のオーディオデータであれば「０ｘ０３」という値に設定され、ＩＳＯ／ＩＥＣ１３８１８－３規格のオーディオデータであれば「０ｘ０４」という値に設定される。このｓｔｒｅａｍ＿ｔｙｐｅは、このプログラムマップセクション中において、ｐｒｏｇｒａｍ＿ｎｕｍｂｅｒで規定されたプログラムを構成するエレメントの数だけ繰返し記述されている。

ｅｌｅｍｅｎｔａｒｙ＿ＰＩＤは、ｐｒｏｇｒａｍ＿ｎｕｍｂｅｒで規定されたプログラムを構成するエレメントを伝送するトランスポートストリームパケットのＰＩＤを指定するためのフィールドである。このｅｌｅｍｅｎｔａｒｙ＿ＰＩＤは、ストリームのエレメントのタイプを示すｓｔｒｅａｍ＿ｔｙｐｅと対応付けられて記述されているデータである。

ＥＳ＿ｉｎｆｏ＿ｌｅｎｇｔｈは、このフィールドＥＳ＿ｉｎｆｏ＿ｌｅｎｇｔｈの次に記述されているディスクリプタのバイト数を規定するためのデータである。

次に、図１７及び図１８を参照して、条件付きアクセステーブル（ＣＡＴ）に

ついて詳細に説明する。この条件付きアクセステーブルは、有料放送において、ビデオデータやオーディオデータに対して施されたスクランブルを解除するためのに使用される受信契約情報ＥＭＭを伝送するパケットのＰＩＤを規定するためのセクションである。また、この条件付きアクセステーブルは、受信契約者だけにプログラムのスクランブルが解除できるようにするための限定受信システム（ＣＡシステム：Ｃｏｎｄｉｔｉｏｎａｌ　Ａｃｃｅｓｓ　Ｓｙｓｔｅｍ）と、受信契約情報ＥＭＭとの関係を規定するためのセクションでもある。

この条件付きアクセステーブルのＰＩＤは、プログラムマップテーブルのようにプログラムアソシエーションテーブルによって指定されるのでは無く、この条件付きアクセステーブルに対して割当てられた固有のＰＩＤ値「０ｘ０１」をビットストリーム中から探し出すことによって、この条件付きアクセステーブルの各フィールドをデコードすることができる。

具体的には、この条件付きアクセステーブルは、ｔａｂｌｅ＿ｉｄと、ｓｅｃｔｉｏｎ＿ｓｙｎｔａｘ＿ｉｎｄｉｃａｔｏｒと、ｓｅｃｔｉｏｎ＿ｌｅｎｇｔｈと、ｖｅｒｓｉｏｎ＿ｎｕｍｂｅｒと、ｃｕｒｒｅｎｔ＿ｎｅｘｔ＿ｉｎｄｉｃａｔｏｒと、ｓｅｃｔｉｏｎ＿ｎｕｍｂｅｒと、ｌａｓｔ＿ｓｅｃｔｉｏｎ＿ｎｕｍｂｅｒと、ｄｉｓｃｒｉｐｔｏｒ（）とから構成されている。

ｔａｂｌｅ＿ｉｄは、各テーブルに対して割当てられた固有の識別番号であって、この条件付きアクセステーブルＣＡＴに割り当てられたｔａｂｌｅ＿ｉｄは「０ｘ０１」である。は「０ｘ０２」である。

ｓｅｃｔｉｏｎ＿ｓｙｎｔａｘ＿ｉｎｄｉｃａｔｏｒは、「１」に固定された定数である。　ｓｅｃｔｉｏｎ＿ｌｅｎｇｔｈは、このｓｅｃｔｉｏｎ＿ｌｅｎｇｔｈの後のビットからＣＲＣセクションの最後のバイトまでのバイト数を示すフィールドである。　ｖｅｒｓｉｏｎ＿ｎｕｍｂｅｒは、条件付きアクセステーブル（ＣＡＴ）のバージョン番号を示すデータである。このｖｅｒ－ｓｉｏｎ＿ｎｕｍｂｅｒは、条件付きアクセステーブルの設定が変更されたとき

に、１づつインクリメントされる。　ｃｕｒｒｅｎｔ＿ｎｅｘｔ＿ｉｎｄｉ－ｃａｔｏｒは、伝送されている条件付きアクセステーブルが現在使用可能であるか否かを示すデータである。条件付きアクセステーブルが現在使用可能であれば、このｃｕｒｒｅｎｔ＿ｎｅｘｔ＿ｉｎｄｉｃａｔｏｒは「１」にセットされ、条件付きアクセステーブルが現在使用可能でないならば、このｃｕｒｒｅｎｔ＿ｎｅｘｔ＿ｉｎｄｉｃａｔｏｒは「０」にセットされる。

ｓｅｃｔｉｏｎ＿ｎｕｍｂｅｒは、この条件付きアクセステーブルのセクション番号を示すデータである。例えば、条件付きアクセステーブルに含まれるＣＡ＿ｓｅｃｔｉｏｎ（）は、最初のセクションであることを示すために、「０ｘ００」に設定される。この条件付きアクセステーブルに含まれるセクションが増える毎に、このｓｅｃｔｉｏｎ＿ｎｕｍｂｅｒは１づつインクリメントされていく。

ｌａｓｔ＿ｓｅｃｔｉｏｎ＿ｎｕｍｂｅｒは、この条件付きアクセステーブルによって規定されている全てのセクションの中で最後のセクションのセクション番号を示すデータである。

ｄｅｓｃｒｉｐｔｏｒ（）は、既に説明したように、プログラム及びプログラムエレメントの定義を拡張するために使用されるデータ構造である。本発明のデータ伝送装置においては、この条件付きアクセステーブルの中でこのｄｅ－ｓｃｒｉｐｔｏｒ（）が使用去れる場合には、このｄｅｓｃｒｉｐｔｏｒ（）は、受信契約情報ＥＭＭを含むパケットのＰＩＤを指定するための情報を記述するために使用されている。

次に、図１９を参照して、プログラムマップテーブル及び条件付きアクセステーブル中で使用される条件付きアクセスディスクリプタＣＡ＿ｄｅｓｃｒｉｐ－ｔｏｒ（）に関して説明する。

条件付きアクセスディスクリプタは、受信契約に関する個人情報及び暗号化されたＥＣＭデータを解読するためのワークキーＫｗを含んだ受信契約情報ＥＭＭおよびビデオやオーディオ等のエレメンタリーストリームに対して施したスクラ

ンブルを解除するためのスクランブルキーＫｓを含んだ番組解読情報ＥＣＭ等を規定するために使用される。従って、ビデオやオーディオ等のエレメンタリーストリームがスクランブルされている場合には、ビットストリーム中に、必ずこの条件付きアクセスディスクリプタが存在する。

条件付きアクセスディスクリプタＣＡ＿ｄｅｓｃｒｉｐｔｏｒ（）は、ｄｅ－ｓｃｒｉｐｔｏｒ＿ｔａｇ、ｄｅｓｃｒｉｐｔｏｒ＿ｌｅｎｇｔｈ、ＣＡ＿ｓｙｓｔｅｍ＿ＩＤ、ＣＡ＿ＰＩＤ、及びｐｒｉｖａｔｅ＿ｄａｔａ＿ｂｙｔｅとから構成されるデータである。ｄｅｓｃｒｉｐｔｏｒ＿ｔａｇは、すでに説明した複数のディスクリプタを識別するための固有の識別タグである。条件付きアクセスディスクリプタＣＡ＿ｄｅｓｃｒｉｐｔｏｒ（）は、このｄｅｓｃｒｉｐ－ｔｏｒ＿ｔａｇとして、「９」が割当てられている。ｄｅｓｃｒｉｐｔｏｒ＿ｌｅｎｇｔｈは、このｄｅｓｃｒｉｐｔｏｒ＿ｌｅｎｇｔｈの直後に続くディスクリプタのデータバイト数を規定するためのデータである。ＣＡ＿ｓｙｓｔｅｍ＿ＩＤは、関連するＥＣＭ又はＥＭＭデータを生成及び適用した限定受信システム（ＣＡシステム）の種類を示すデータである。ＣＡ＿ＰＩＤは、ＣＡ＿ｓｙｓｔｅｍ＿ＩＤによって規定される限定受信システム（ＣＡシステム）についてのＥＣＭ又はＥＭＭデータを含んでいるトランスポートストリームのＰＩＤを示す。

条件付きアクセスディスクリプタＣＡ＿ｄｅｓｃｒｉｐｔｏｒ（）のＣＡ＿ＰＩＤによって指定されるパケットに記述されているデータ内容は、このＣＡ＿ｄｅｓｃｒｉｐｔｏｒ（）のコンテキスト（文脈）によって異なってくる。図２０を参照して、このＣＡ＿ＰＩＤが指定するパケットについて説明する。

まず、ＣＡ＿ＰＩＤによって指定されるパケットに記述されているデータ内容は、このＣＡ＿ｄｅｓｃｒｉｐｔｏｒ（）が、条件付きアクセステーブルＣＡＴで使用されているかプログラムマップテーブルにおいて使用されているかによって異なってくる。具体的には、ＣＡ＿ｄｅｓｃｒｉｐｔｏｒ（）が条件付きアクセステーブルに存在する場合には、ＣＡ＿ＰＩＤは、ＥＭＭデータが含まれるト

ランスポートストリームのパケットを示す。ＣＡ＿ｄｅｓｃｒｉｐｔｏｒ（）がプログラムマップテーブルに存在する場合には、ＣＡ＿ＰＩＤは、ＥＣＭデータが含まれるトランスポートストリームのパケットを示す。

さらに、ＣＡ＿ＰＩＤによって指定されるパケットに記述されているデータ内容は、条件付きアクセスディスクリプタＣＡ＿ｄｅｓｃｒｉｐｔｏｒ（）のプログラムマップテーブル内のコンテキストに応じても、データ内容が異なってくる。この件付きアクセスディスクリプタＣＡ＿ｄｅｓｃｒｉｐｔｏｒ（）のプログラムマップテーブル内のコンテキストとは、このＣＡ＿ｄｅｓｃｒｉｐｔｏｒ（）が、最初のｆｏｒ文内（図１５）において使用されているディスクリプタで使用されているか第２番めのｆｏｒ文内（図１５）において使用されているかということである。

この条件付きアクセスディスクリプタＣＡ＿ｄｅｓｃｒｉｐｔｏｒ（）が、最初のｆｏｒ文内で使用されている場合には、ＣＡ＿ＰＩＤは、ＥＣＭデータが含まれるトランスポートストリームパケットのＰＩＤを示す。つまり、この場合、この第１のＣＡ＿ｄｅｓｃｒｉｐｔｏｒ（）は、ｐｒｏｇｒａｍ＿ｎｕｍｂｅｒで規定されたプログラムが含まれるトランスポートストリームパケットとＥＣＭデータが含まれるトランスポートストリームパケットとの対応を記述するためのシンタックスである。つまり、ｐｒｏｇｒａｍ＿ｎｕｍｂｅｒで規定されたプログラムに含まれる全てのデータエレメントに対して、同じＥＣＭデータが割り当てられているということである。言い換えると、プログラムに含まれる全てのデータエレメントに対して同じスクランブルキーを使用してスクランブル処理及びデスクランブル処理が行われていることを示す。

一方、この条件付きアクセスディスクリプタＣＡ＿ｄｅｓｃｒｉｐｔｏｒ（）が、第２番めのｆｏｒ文内で使用されている第２のＣＡ＿ｄｅｓｃｒｉｐｔｏｒ（）である場合には、同じように、ＣＡ＿ＰＩＤは、ＥＣＭデータが含まれるトランスポートストリームパケットのＰＩＤを示す。しかしながら、この第２のＣＡ＿ｄｅｓｃｒｉｐｔｏｒ（）は、ｐｒｏｇｒａｍ＿ｎｕｍｂｅｒで規定された

プログラム含まれるトランスポートストリームパケットとＥＣＭデータが含まれるトランスポートストリームパケットとの対応を記述しているのではなく、このＣＡ＿ｄｅｓｃｒｉｐｔｏｒ（）は、ｅｌｅｍｅｎｔａｒｙ＿ＰＩＤで規定されたデータエレメントが含まれるトランスポートストリームパケットと、ＥＣＭデータが含まれるトランスポートストリームパケットとの対応を記述している。つまり、ｅｌｅｍｅｎｔａｒｙ＿ＰＩＤで規定されたデータエレメント毎に、ＥＣＭデータが割り当てられているということである。言い換えると、プログラムに含まれるデータエレメント毎に異なるスクランブルキーを使用してスクランブル処理及びデスクランブル処理が行われていることを示す。このように、データエレメント毎に異なるスクタンブルキーを使用するということは、例えば、１チャンネルのビデオデータと主音声と副音声からなる２チャンネルのオーディオデータから成るプログラムを想定した場合に、副音声のみに異なるスクランブルキーを使用してスクランブルをかけることができる。

次にＥＭＭデータ及びＥＣＭデータについて説明する。

ＥＭＭ（Ｅｎｔｉｔｌｅｍｅｎｔ　Ｍａｎａｇｅｍｅｎｔ　Ｍｅｓｓａｇｅ）データは、視聴者が契約した番組等を示す契約情報やスクランブキーＫｓを暗号化するために使用したワークキーＫｗを含んだデータである。ＥＭＭデータは、プログラムアソシエーションテーブルＰＡＴやプログラムマップテーブルＰＭＴや条件付きアソシエーションテーブルＣＡＴと同じように、トランスポートストリームパケットのペイロードに挿入されて伝送される。以下の説明において、このＥＭＭデータを含むトランスポートストリームパケットを、ＥＭＭパケットと呼ぶことにする。

ＥＭＭパケットは、図２１のように、４バイトのヘッダと、１８３バイトのペイロード部とから構成されている。ＥＭＭパケットのヘッダは、すでに説明したトランスポートストリームのパケットと同じように、ｓｙｎｃ＿ｂｙｔｅ、ｔｒａｎｓｐｏｒｔ＿ｅｒｒｏｒ＿ｉｎｄｉｃａｔｏｒ、ｐａｙｌｏａｄ＿ｕｎｉｔ＿ｓｔａｒｔ＿ｉｎｄｉｃａｔｏｒ、ｔｒａｎｓｐｏｒｔ＿ｐｒｉ－

ｏｒｉｔｙ、ＰＩＤ、ｔｒａｎｓｐｏｒｔ＿ｓｃｒａｍｂｌｉｎｇ＿ｃｏｎ－ｔｒｏｌ、ａｄａｐｔａｔｉｏｎ＿ｆｉｅｌｄ＿ｃｏｎｔｒｏｌ、及びｃｏｎ－ｔｉｎｕｉｔｙ＿ｃｏｕｎｔｅｒ等のデータフィールドから構成されている。１８３バイトのペーロード部は、ＥＭＭセクションヘッダ部と、ＥＭＭデータ部と、ＣＲＣ部と、スタッフィングバイト部とから構成されている。

ＥＭＭセクションヘッダは、ｔａｂｌｅ＿ｉｄ、ｓｅｃｔｉｏｎ＿ｓｙｎ－ｔａｘ＿ｉｎｄｉｃａｔｏｒ、ｒｅｓｅｒｖｅｄ＿０、ｒｅｓｅｒｖｅｄ＿１、ｓｅｃｔｉｏｎ＿ｌｅｎｇｔｈ、ｔａｂｌｅ＿ｉｄ＿ｅｘｔｅｎｔｉｏｎ、ｒｅｓｅｒｖｅｄ＿２、ｖｅｒｓｉｏｎ＿ｎｕｍｂｅｒ、ｃｕｒｒｅｎｔ＿ｎｅｘｔ＿ｉｎｄｉｃａｔｏｒ、ｓｅｃｔｉｏｎ＿ｎｕｍｂｅｒ、及びｌａｓｔ＿ｓｅｃｔｉｏｎ＿ｎｕｍｂｅｒ等のデータフィールドから構成されている。ｔａｂｌｅ＿ｉｄは、各テーブル（各セクション）に対して割当てられた固有の識別番号である。このＥＭＭセクションの識別番号としては、「０ｘ４０」から「０ｘＦＥ」までのユーザ定義可能なｔａｂｌｅ＿ｉｄが割当てられている。ｓｅｃｔｉｏｎ＿ｓｙｎｔａｘ＿ｉｎｄｉｃａｔｏｒは、「１」に固定された定数である。ｓｅｃｔｉｏｎ＿ｌｅｎｇｔｈは、このｓｅｃｔｉｏｎ＿ｌｅｎｇｔｈの後のビットからＣＲＣセクションの最後のバイトまでのバイト数を示すデータフィールドである。ｔａｂｌｅ＿ｉｄ＿ｅｘｔｅｎｔｉｏｎは、このＥＭＭセクションの拡張データがあるか無いかを示すデータである。ｖｅｒ－ｓｉｏｎ＿ｎｕｍｂｅｒは、ＥＭＭセクションのバージョン番号を示すデータである。トランスポートストリームにおいてこのＥＭＭセクションのパラメータが変化する場合にこのバーション番号がインクリメントされる。ｃｕｒｒｅｎｔ＿ｎｅｘｔ＿ｉｎｄｉｃａｔｏｒは、伝送されているＥＭＭセクションが現在使用可能であるか否かを示すデータである。ｓｅｃｔｉｏｎ＿ｎｕｍｂｅｒは、このＥＭＭセクションの番号を示すデータであって、常に、「１」である。ＥＭＭｌａｓｔ＿ｓｅｃｔｉｏｎ＿ｎｕｍｂｅｒは、このＥＭＭセクションの中で最後のセクションのセクション番号を示すデータであって、常に「１」である。

ＥＭＭデータ部は、ｃａｒｄ＿ＩＤ、ＥＭＭ＿ｔｙｐｅ、ＣＡ＿ｓｙｓｔｅｍ＿ＩＤ、Ｋｗ＿Ｎｏ、Ｋｗ、ａｕｔｈｏｒｉｚｅ＿ｔｙｐｅ、ｓｅｒｖｉｃｅ＿ＩＤ、ｓｅｒｉｅｓ＿ＩＤ、ｅｖｅｎｔ＿ＩＤ、及びｃｏｍｐｏｎｅｎｔ＿ｍａｐ等のデータフィールドから構成されている。

ｃａｒｄ＿ＩＤは、ＩＲＤにセットされた固有のＩＣカードに付与された識別番号であって、この顧客を管理するための識別番号としても使用されている。ＥＭＭ＿ｔｙｐｅは、ＥＭＭデータの種類を示すデータである。ＣＡ＿ｓｙｓｔｅｍ＿ＩＤは、顧客管理システムを含むＣＡシステムに付与された識別番号である。Ｋｗは、スクランブルキーＫｓを暗号化するために使用したワークキーを示し、Ｋｗ＿Ｎｏは、予め登録された２５６個のワークキーＫｗのうち、スクランブルキーＫｓを暗号化する際に使用されたワークキーがどのワークキーであるかを示す番号である。ａｕｔｈｏｒｉｚｅ＿ｔｙｐｅ、ｓｅｒｖｉｃｅ＿ＩＤ、ｓｅｒｉｅｓ＿ＩＤ及びｅｖｅｎｔ＿ＩＤは、視聴者がどの番組を契約しているかを示す契約条件である。ｃｏｍｐｏｎｅｎｔ＿ｍａｐは、契約しているプログラムを構成するエレメントにおいて、どのエレメントの契約がなされているかをエレメント毎に示すデータである。

ＥＣＭ（Ｅｎｔｉｔｌｅｍｅｎｔ＿Ｃｏｎｔｒｏｌ＿Ｍｅｓｓａｇｅ）データは、視聴者が契約したプログラムに施されたスクランブルを解除するためのスクランブルキーＫｓを含んだデータである。ＥＣＭデータは、プログラムアソシエーションテーブルＰＡＴやプログラムマップテーブルＰＭＴや条件付きアソシエーションテーブルＣＡＴと同じように、トランスポートストリームパケットのペイロードに挿入されて伝送される。以下の説明において、このＥＣＭデータを含むトランスポートストリームパケットを、ＥＣＭパケットと呼ぶことにする。ＥＣＭパケットは、約１００ｍｓｅｃの周期で伝送され、ＥＭＭデータとして伝送されるスクランブルキーは、約４秒毎に新しく更新されるようになっている。

ＥＣＭパケットは、図２２のように、４バイトのヘッダと、１８３バイトのペイロード部とから構成されている。ＥＣＭパケットのヘッダは、すでに説明した

トランスポートストリームのパケットと同じように、ｓｙｎｃ＿ｂｙｔｅ、ｔｒａｎｓｐｏｒｔ＿ｅｒｒｏｒ＿ｉｎｄｉｃａｔｏｒ、ｐａｙｌｏａｄ＿ｕｎｉｔ＿ｓｔａｒｔ＿ｉｎｄｉｃａｔｏｒ、ｔｒａｎｓｐｏｒｔ＿ｐｒｉｏｒｉｔｙ、ＰＩＤ、ｔｒａｎｓｐｏｒｔ＿ｓｃｒａｍｂｌｉｎｇ＿ｃｏｎｔｒｏｌ、ａｄａｐｔａｔｉｏｎ＿ｆｉｅｌｄ＿ｃｏｎｔｒｏｌ、及びｃｏｎｔｉｎｕｉｔｙ＿ｃｏｕｎｔｅｒ等のデータフィールドから構成されている。１８３バイトのペーロード部は、ＥＣＭセクションヘッダ部と、ＥＣＭデータ部と、ＣＲＣ部と、スタッフィングバイト部とから構成されている。

ＥＣＭセクションヘッダは、ｔａｂｌｅ＿ｉｄ、ｓｅｃｔｉｏｎ＿ｓｙｎｔａｘ＿ｉｎｄｉｃａｔｏｒ、ｒｅｓｅｒｖｅｄ＿０、ｒｅｓｅｒｖｅｄ＿１、ｓｅｃｔｉｏｎ＿ｌｅｎｇｔｈ、ｔａｂｌｅ＿ｉｄ＿ｅｘｔｅｎｔｉｏｎ、ｒｅｓｅｒｖｅｄ＿２、ｖｅｒｓｉｏｎ＿ｎｕｍｂｅｒ、ｃｕｒｒｅｎｔ＿ｎｅｘｔ＿ｉｎｄｉｃａｔｏｒ、ｓｅｃｔｉｏｎ＿ｎｕｍｂｅｒ、及びｌａｓｔ＿ｓｅｃｔｉｏｎ＿ｎｕｍｂｅｒ等のデータフィールドから構成されている。ｔａｂｌｅ＿ｉｄは、各テーブル（各セクション）に対して割当てられた固有の識別番号である。このＥＣＭセクションの識別番号としては、「０ｘ４０」から「０ｘＦＥ」までのユーザ定義可能なｔａｂｌｅ＿ｉｄが割当てられている。ｓｅｃｔｉｏｎ＿ｓｙｎｔａｘ＿ｉｎｄｉｃａｔｏｒは、「１」に固定された定数である。ｓｅｃｔｉｏｎ＿ｌｅｎｇｔｈは、このｓｅｃｔｉｏｎ＿ｌｅｎｇｔｈの後のビットからＣＲＣセクションの最後のバイトまでのバイト数を示すデータフィールドである。ｔａｂｌｅ＿ｉｄ＿ｅｘｔｅｎｔｉｏｎは、このＥＣＭセクションの拡張データがあるか無いかを示すデータである。ｖｅｒｓｉｏｎ＿ｎｕｍｂｅｒは、ＥＣＭセクションのバージョン番号を示すデータである。トランスポートストリームにおいてこのＥＣＭセクションのパラメータが変化する場合にこのバーション番号がインクリメントされる。ｃｕｒｒｅｎｔ＿ｎｅｘｔ＿ｉｎｄｉｃａｔｏｒは、伝送されているＥＣＭセクションが現在使用可能であるか否かを示すデータである。ｓｅｃｔｉｏｎ＿ｎｕｍｂｅｒは、この

ＥＣＭセクションの番号を示すデータであって、常に、「１」である。ＥＣＭｌａｓｔ＿ｓｅｃｔｉｏｎ＿ｎｕｍｂｅｒは、このＥＣＭセクションの中で最後のセクションのセクション番号を示すデータであって、常に「１」である。

ＥＣＭデータ部は、ＥＣＭ＿ｔｙｐｅ、ＣＡ＿ｓｙｓｔｅｍ＿ＩＤ、Ｋｗ＿Ｎｏ、ｓｅｒｖｉｃｅ＿ｍｏｄｅ、ｓｅｒｖｉｃｅ＿ＩＤ、ｓｅｒｉｅｓ＿ＩＤ、ｅｖｅｎｔ＿ＩＤ、ｃｏｍｐｏｎｅｎｔ＿ｍａｐ、Ｋｓ＿Ｏｄｄ及びＫｓ＿Ｅｖｅｎ等のデータフィールドから構成されている。

ＥＣＭ＿ｔｙｐｅは、ＥＣＭデータの種類を示すデータである。ＣＡ＿ｓｙｓｔｅｍ＿ＩＤは、顧客管理システムを含むＣＡシステムに付与された識別番号である。Ｋｗ＿Ｎｏは、予め登録された２５６個のワークキーＫｗのうち、スクランブルキーＫｓを暗号化する際に使用されたワークキーがどのワークキーであるかを示す番号である。ｓｅｒｖｉｃｅ＿ｍｏｄｅ、ｓｅｒｖｉｃｅ＿ＩＤ、ｓｅｒｉｅｓ＿ＩＤ及びｅｖｅｎｔ＿ＩＤは、視聴者がどの番組を契約しているかを示す契約条件である。ｃｏｍｐｏｎｅｎｔ＿ｍａｐは、契約しているプログラムを構成するエレメントにおいて、どのエレメントの契約がなされているかをエレメント毎に示すデータである。Ｋｓ＿Ｏｄｄ及びＫｓ＿Ｅｖｅｎは、伝送されたビデオデータ及びオーディオデータをスクランブルするために使用したスクランブルキーである。スクランブルキーは、奇数キーＫｓ＿Ｏｄｄと偶数キーＫｓ＿Ｅｖｅｎから構成され、奇数キーと遇数キーとが４秒毎に交互にスクランブルーとして使用される。

次に、図２３を参照して、受信機として設けられたＩＲＤ（Ｉｎｔｅ－ｇｒａｔｅｄ＿Ｒｅｃｅｉｖｅｒ＿Ｄｅｃｏｄｅｒ）２０について詳細に説明する。

このＩＲＤは、衛星を介して伝送された変調ストリームを復調するための復調回路２１と、復調回路２１において復調されたストリームをパケットの種類に応じて分離するデマルチプレクサ２２と、デマルチプレクサ２２によって分離されたＰＡＴパケット、ＰＭＴパケット、ＣＡＴパケット、ＥＭＭパケット、及びＥ

ＣＭパケットを受け取るＣＰＵ２３と、暗号化ワークキーＫｗ’と暗号化スクランブルキーＫｓ’の暗号を解読するためのセキュリティモジュール２４と、スクランブルされたビデオストリーム、オーディオストリーム及びプライベートデータストリームのスクランブルを解除するデスクランブラー２５Ｖ、２５Ａ及び２５Ｐと、ビデオストリーム及びオーディオストリームを復号化するデコーダ２６Ｖ、２６Ａとを有している。

デマルチプレクサ２２は、ＣＰＵ２３から制御コマンドを受取り、このコマンドに応答して適切なトランスポートストリームパケットを適切なタイミングでＣＰＵ２３に供給する機能を有している。

ＣＰＵ２３は、デマルチプレクサ２２から供給されたＰＡＴパケットを解析するＰＡＴパケット解析部２３１と、デマルチプレクサ２２から供給されたＰＭＴパケットを解析するＰＭＴパケット解析部２３２と、デマルチプレクサ２２から供給されたＣＡＴパケットを解析するＣＡＴパケット解析部２３３、デマルチプレクサ２２から供給されたＥＭＭ’パケットを解析するＥＭＭパケット解析部２３４と、デマルチプレクサ２２から供給されたＥＣＭ’パケットを解析するＥＣＭパケット解析部２３５とを有している。

ＰＡＴ解析部２３１は、デマルチプレクサ２２からＰＡＴパケットとして供給されたトランスポートストリームパケットを解析することによって、このＰＡＴパケットに含まれているｐｒｏｇｒａｍ＿ｎｕｍｂｅｒとｐｒｏｇｒａｍ＿ｍａｐ＿ＰＩＤを得る。また、ＰＡＴ解析部２３１は、セキュリティモジュール２４から受信者が契約しているプログラムがどのプログラムであるかを示すａｕｔｈｏｒｉｚｅ＿ｔｙｐｅを受け取る。そして、ＰＡＴ解析部２３１は、セキュリティモジュールから供給されたａｕｔｈｏｒｉｚｅ＿ｔｙｐｅとデマルチプレクサ２２から供給されたｐｒｏｇｒａｍ＿ｎｕｍｂｅｒとを比較し、視聴者が契約しているプログラムと一致したｐｒｏｇｒａｍ＿ｎｕｍｂｅｒに対応したｐｒｏｇｒａｍ＿ｍａｐ＿ＰＩＤのみを選択する。その結果、ＰＡＴ解析部２３１は、視聴者が契約しているプログラムに対応したプログラムマップテーブルの

ＰＩＤのみを得ることができる。

続いて、デマルチプレクサ２２は、ＰＡＴ解析部２３１から供給されたｐｒｏｇｒａｍ＿ｍａｐ＿ＰＩＤによって指定されたＰＩＤを有したトランスポートストリームパケットを選択し、その選択されたトランスポートストリームパケットをＰＭＴパケットとしてＰＭＴ解析部２３２に出力する。

ＰＭＴ解析部２３２は、ｐｒｏｇｒａｍ＿ｍａｐ＿ＰＩＤによって指定されたＰＩＤを有したＭＰＴパケットに含まれるＰＭＴデータを解析する。具体的には、ＰＭＴ解析部２３２は、ＰＭＴパケットのＰＭＴデータとして記述されたｅｌｅｍｅｎｔａｒｙ＿ＰＩＤから、ｐｒｏｇｒａｍ＿ｎｕｍｂｅｒによって指定されたプログラムを構成するデータエレメントが含まれたトランスポートストリームパケットのＰＩＤを得る。例えば、プログラムがビデオデータとオーディオデータの２つのデータエレメントから構成されるとすると、第１のｅｌｅｍｅｎｔａｒｙ＿ＰＩＤによってビデオストリームが含まれるトランスポートストリームパケットを指定し、第２のｅｌｅｍｅｎｔａｒｙ＿ＰＩＤによってオーディオストリームが含まれるトランスポートストリームパケットを指定するということである。

さらに、このＰＭＴ解析部２３２は、ＰＭＴデータ中にｄｅｓｃｒｉｐｔｏｒ（）関数として記述されたＣＡ＿ｄｅｓｃｒｉｐｔｏｒを参照する。そして、このＰＭＴ解析部２３２は、このＣＡ＿ｄｅｓｃｒｉｐｔｏｒ中に記述されたＣＡ＿ＰＩＤを得て、このＣＡ＿ＰＩＤをデマルチプレクサ２２にフィードバックする。このＣＡ＿ｄｅｓｃｒｉｐｔｏｒ中に記述されたＣＡ＿ＰＩＤは、ＥＣＭデータが含まれたトランスポートストリームパケットのＰＩＤを示すデータである。

続いて、デマルチプレクサ２２は、ＰＭＴ解析部２３２から供給された、ｅｌｅｍｅｎｔａｒｙ＿ＰＩＤによって指定されたＰＩＤを有したトランスポートストリームパケットを適切な処理回路に出力する。例えば、データエレメントがビデオストリームであれば、ビデオストリームをデスクランブするためのデス

クランブル回路２５Ｖに出力し、データエレメントがオーディオストリームであれば、オーディオストリームをデスクランブルするためのデスクランブル回路２５Ａに出力し、データエレメントがプライベートデータストリームであれば、プライベートデータストリームをデスクランブルするためのデスクランブル回路２５Ｐに出力する。

さらに、デマルチプレクサ２２は、ＣＡ＿ＰＩＤによって指定されたＰＩＤを有したトランスポートストリームパケットを、ＥＣＭパケットとしてＥＣＭ解析部２３５に供給する。よって、ＥＣＭ解析部２３５に供給されるＥＣＭデータは、視聴者が契約しているプログラムに関するＥＣＭデータのみである。

ＥＣＭ解析部２３５は、まず、デマルチプレクサ２２から受け取ったＥＣＭ'パケットをフィルタリングする。具体的には、ＥＣＭ解析部２３５は、このＥＣＭデータ部内のＣＡ＿ｓｙｓｔｅｍ＿ＩＤとセキュリティモジュール２４から供給されたＣＡ＿ｓｙｓｔｅｍ＿ＩＤとを比較し、セキュリティモジュール２４から供給されたＣＡ＿ｓｙｓｔｅｍ＿ＩＤと一致するＣＡ＿ｓｙｓｔｅｍ＿ＩＤとを含んだＥＣＭパケットのみを選択する。次に、ＥＣＭ解析部２３５は、この選択されたＥＣＭパケットに含まれるＥＣＭデータを解析することによって、暗号化スクランブルキーｋｓ'を得ることができる。ＥＣＭ解析部２３５は、この暗号化スクランブルキーＫｓ'を、セキュリティモジュール２４内のマイクロプロセッサＭＰＵ内の暗号解読回路２４２に供給する。

一方、デマルチプレクサ２２は、伝送されたビットストリーム中から、ＣＡＴパケットのＰＩＤを有したトランスポートストリームパケットを検出し、その検出したトランスポートストリームパケットをＣＡＴパケットとしてＣＡＴ解析部２３３に出力する。

ＣＡＴ解析部２３３は、まず、デマルチプレクサ２２から受け取ったＣＡＴパケットに含まれるＣＡ＿ｄｅｓｃｒｉｐｔｏｒ（）関数を検出し、ＣＡ＿ｄｅｓｃｒｉｐｔｏｒ（）関数内のＣＡ＿ＰＩＤから、ＣＡＴパケットのＣＡ＿ｄｅｓｃｒｉｐｔｏｒ（）によって指定されたトランスポートストリームパケッ

トのＰＩＤを得る。このＣＡＴパケットのＣＡ＿ｄｅｓｃｒｉｐｔｏｒ（）によって指定されたトランスポートストリームパケットが、ＥＭＭ情報を含んだトランスポートストリームパケットである。

デマルチプレクサ２２は、ビットストリーム中から、ＣＡＴ解析部２３３から受け取ったＣＡ＿ＰＩＤによって指定されたＰＩＤを有したトランスポートストリームパケットを選択して、その選択されたトランスポートストリームパケットをＥＭＭ’パケットとしてＥＭＭ解析部２３４に供給する。

ＥＭＭ解析部２３４は、まず、デマルチプレクサ２１２から受け取ったＥＭＭ’パケットをフィルタリングして、このセキュティモジュールに対応したＥＭＭ’パケットのみを選択する。具体的には、デマルチプレクサ２２から受け取ったＥＭＭパケットのＣＡ＿ｄｅｓｃｒｉｐｔｏｒ（）のＣＡ＿ＰＩＤによって指定されたトランスポートストリームパケットは、ＥＭＭデータを含んだ全てのＥＭＭ’パケットであるので、このＣＡ＿ＰＩＤを参照することによって、ＥＭＭ’パケットに含まれるＥＭＭデータを得ることができる。ＥＭＭ解析部２３４は、このＥＭＭデータ部内のＣａｒｄ＿ＩＤとＣＡ＿ｓｙｓｔｅｍ＿ＩＤと、セキュリティモジュール２４のメモリ２４１から供給されたＣａｒｄ＿ＩＤとＣＡ＿ｓｙｓｔｅｍ＿ＩＤとを比較し、セキュリティモジュール２４から供給されたＣａｒｄ＿ＩＤとＣＡ＿ｓｙｓｔｅｍ＿ＩＤとそれぞれ一致するＣａｒｄ＿ＩＤとＣＡ＿ｓｙｓｔｅｍ＿ＩＤとを含んだＥＭＭ’パケットのみを選択する。

次に、ＥＭＭ解析部２３４は、この選択したＥＭＭパケットに含まれる１０１バイトのＥＭＭデータを、最新のＥＭＭデータとしてセキュリティモジュール２４のメモリ２４１に供給し、メモリ２４１内の古いＥＭＭデータを更新する。さらに、ＥＭＭ解析部２３４は、このＥＭＭデータに含まれる暗号化ワークキーＫｗ’を、セキュリティモジュール２４内のマイクロプロセッサＭＰＵ内の暗号解読回路２４２に供給する。

セキュリティモジュール２４は、メモリ２４１と第１の暗号解読回路２４２及び第２の暗号解読回路２４３を備えたマイクロプロセッサとから構成されている

。このセキュリティモジュール２４は、例えば、ＩＲＤ本体に対して着脱可能なＩＣカードで構成されている。

セキュリティモジュール２４の第１の暗号解読回路２４２は、ＥＭＭ解析部２３４から暗号化ワークキーＫｗ'を受取り、予め記憶されたマスターキーＫｍによってこの暗号化ワークキーＫｗ'の暗号を解読する。そして、第１の暗号解読回路２４２は、この暗号解読されたワークキーＫｗを、暗号化第２の暗号解読回路２４３に供給する。

セキュリティモジュール２４の第２の暗号解読回路２４２は、ＥＣＭ回路２３５から暗号化スクランブルキーＫｓ'を受取ると共に、第１の暗号解読回路２４２から暗号解読されたワークキーＫｗを受取り、この暗号解読されたワークキーＫｗによって、暗号化スクランブルキーＫｓ'の暗号を解読する。暗号解読されたスクランブルキーＫｓは、デスクランブラ２５Ｖ、２５Ａ及び２５Ｐに供給される。ここでは、デスクランブラ２５Ｖ、２５Ａ及び２５Ｐに同じスクランブルキーＫｓを供給する場合について説明したが、もし、各データエレメント毎に異なるスクランブルキーＫｓが設定されている場合には、各デスクランブラに対してそれぞれ異なるスクランブルキーＫｓが供給される。

以上の構成において、トランスポートストリームパケット構成の複数のデータエレメントからなるプログラムデータの上記各トランスポートストリームパケットを多重化して送信するデータ多重化装置において、１つのプログラムを構成する複数のデータエレメントのうち、１つ又は複数のデータエレメントに対応したスクランブルキーを生成し、各データエレメントごとにスクランブルをかけることにより、視聴者はデータエレメントごとに視聴契約を結ぶことができる。

また、多重化された各トランスポートストリームパケットに対してそれぞれ対応するスクランブルキーを用いてスクランブルをかけることにより、各トランスポートストリームパケットを多重化する前にスクランブルをかける場合に比べて、スクランブルをかけるための回路構成が簡単になる。

また、各バッファメモリに入力されるデータエレメントの入力レートが基準レ

ートに比べて高いとき、複数のバッファメモリのうち、優先順位の低い情報をバッファリングするバッファメモリを切り換え対象から除外してスイッチ手段を切り換え制御することにより、優先順位の高いデータエレメントをバッファリングするバッヘァメモリがオーバーフローすることを未然に防止し得る。

また、受信装置側では、スクランブルキーを用いて当該スクランブルキーに対応するデータエレメントごとにそのトランスポートストリームパケットをデスクランブルすることにより、データエレメントごとに個別にスクランブルを解除することができる。

かくして以上の構成によれば、視聴者は必要とするデータエレメントのみを契約して視聴することができるデータ多重化装置を簡単な構成によつて実現できる。

また優先順位の低いデータエレメントを選択対象から除外して必要なデータエレメントを優先的に選択して多重化することにより、バッヘァメモリのオーバーフローを有効に回避することができる。

産業上の利用可能性

本発明は、ＭＰＥＧ２を用いてビデオデータやオーディオデータを圧縮符号化し、その符号化されたストリームを地上波や衛星波を介して放送するデジタル放送システムに利用できる。

請求の範囲

1．トランスポートストリームパケット構成の複数のデータエレメントからなるプログラムデータの上記各トランスポートストリームパケットを多重化して送信するデータ多重化装置において、

上記データエレメントごとに対応するスクランブルキーを生成するスクランブルキー生成手段と、

上記スクランブルキー生成手段によって生成されたスクランブルキーを用いて対応する上記データエレメントのトランスポートストリームパケットにスクランブルをかけるスクランブル手段と

を備えることを特徴とするデータ多重化装置。

2．上記スクランブルキー生成手段は、

上記1つのプログラムを構成する上記複数のデータエレメントのうち、1つ又は複数のデータエレメントに対応したスクランブルキーを生成する

ことを特徴とする請求の範囲第1項に記載のデータ多重化装置。

3．上記プログラムを構成する複数のデータエレメントは、ビデオデータ、メインオーディオデータ、サブオーディオデータ及びプライベートデータである

ことを特徴とする請求の範囲第1項に記載のデータ多重化装置。

4．上記スクランブル手段は、

上記多重化された各トランスポートストリームパケットに対してそれぞれ対応する上記スクランブルキーを用いてスクランブルをかける

ことを特徴とする請求の範囲第1項に記載のデータ多重化装置。

5．上記スクランブル手段は、

上記各トランスポートストリームパケットを表すパケット識別コードとその対応するスクランブルキーとの対応表を用いて上記各トランスポートストリームパケットにスクランブルをかけるための各スクランブルキーを検索する

ことを特徴とする請求の範囲第4項に記載のデータ多重化装置。

6．上記データ多重化装置は、

ワークキーを用いて上記スクランブルキーを暗号化する第1の暗号化手段を具え、上記暗号化されたスクランブルキーを上記各トランスポートストリームパケットと共に多重化して送信する

ことを特徴とする請求の範囲第4項に記載のデータ多重化装置。

7．上記データ多重化装置は、

マスターキーを用いて上記ワークキーを暗号化する第2の暗号化手段を具え、上記暗号化されたワークキーを上記各トランスポートストリームパケットと共に多重化して送信する

ことを特徴とする請求の範囲第6項に記載のデータ多重化装置。

8．複数のデータエレメントを構成する複数のパケットデータを格納する複数のバッファメモリと、

上記バッファメモリを切り換えるスイッチ手段を有し、当該スイッチ手段によつて上記バッファメモリを順次時分割に切り換えることによって上記複数のパケットデータ列を時分割に多重化して出力する多重化手段と、

上記スイッチ手段による切り換え対象である上記複数のバッファメモリを、上記パケットデータ列の入力レートに応じて選択するスイッチ制御手段と

を備えることを特徴とするデータ多重化装置。

9．上記スイッチ制御手段は、

上記入力レートが基準レートに比べて高いとき、上記複数のバッファメモリのうち、優先順位の低い情報をバッファリングするバッファメモリを切り換え対象から除外して上記スイッチ手段を切り換え制御する

ことを特徴とする請求の範囲第８項に記載のデータ多重化装置。

１０．上記スイッチ制御手段は、

ＥＭＭデータを含むパケットデータを上記優先順位の低い情報として上記ＥＭＭデータを含むパケットデータをバッファリングするバッファメモリを上記切り換え対象から除外する

ことを特徴とする請求の範囲第９項に記載のデータ多重化装置。

１１．上記スイッチ制御手段は、

上記ＥＭＭデータを含むパケットデータをバッファリングするバッファメモリを上記切り換え対象から除外した後、上記入力レートが上記基準レートに比べて依然として高いとき、上記ＥＭＭデータを含むパケットデータをバッファリングするバッファメモリに加えて、ＥＰＧデータを含むパケットデータをバッファリングするバッファメモリを上記切り換え対象から除外する

ことを特徴とする請求の範囲第１０項に記載のデータ多重化装置。

１２．複数のデータエレメントから構成されるプログラムを配信するプログラム配信システムにおいて、顧客のプログラム毎及びデータエレメント毎の契約を管理するための顧客管理システムと、上記プログラムに含まれるデータエレメントをデスクランブルする際に使用するスクランブルキーを上記データエレメント毎に生成する視聴許可システムと、

上記複数のプログラムに含まれるデータエレメントをそれぞれ符号化し、その符号化データエレメントから構成される符号化ストリームを上記各プログラム毎に生成する符号化システムと、上記符号化手段から各プログラム毎に出力された

符号化ストリームを多重化する多重化手段と、上記視聴許可システムにおいて生成されたスクランブルキーに基いて、上記多重化ストリームに含まれる符号化データエレメントに対して各データエレメント毎に選択的にスクランブルをかけるスクランブル手段とを備えたマルチプレクサシステムと、

を備えたことを特徴とするプログラム配信システム。

１３．上記顧客管理システムは、

上記スクランブルキーを暗号化するためのワークキーを生成し、

上記顧客を識別するための顧客識別番号及び上記ワークキーを、ＥＭＭデータとして上記視聴許可システムに供給することを特徴とする請求の範囲第１２項に記載のプログラム配信システム。

１４．上記視聴許可システムは、

上記ＥＭＭデータとして供給されたワークキーを、マスターキーを使用して暗号化し、暗号化ワークキーを出力する第１の暗号化手段を有していることを特徴とする請求の範囲第１３項に記載のプログラム配信システム。

１５．上記視聴許可システムは、

上記第１の暗号化手段によって暗号化された暗号化ワークキー及び上記顧客識別番号を、暗号化ＥＭＭデータとして上記マルチプレクサシステムに供給することを特徴とする請求の範囲第１４項に記載のプログラム配信システム。

１６．上記視聴許可システムは、

上記第１の暗号化手段において暗号化された暗号化ワークキーを識別するためのワークキー識別番号と、上記スクランブルキーとをＥＣＭデータとして上記マルチプレクサシステムに供給することを特徴とする請求の範囲第１５項に記載のプログラム配信システム。

１７．上記視聴許可システムは、

上記ワークキーと、該ワークキーを識別するためのワークキー識別番号とをそれぞれ対応付けて登録したワークキーテーブルを備え、

該ワークキーテーブルを上記マルチプレクサシステムに供給することを特徴とする請求の範囲第１６項に記載のプログラム配信システム。

１８．上記マルチプレクサシステムは、

上記ＥＣＭデータに含まれるスクランブルキーを上記ワークキーを使用して暗号化し、暗号化スクランブルキーを出力するための第２の暗号化手段を有していることを特徴とする請求の範囲第１７項に記載のプログラム配信システム。

１９．上記第２の暗号化手段は、

上記スクランブルキーを暗号化するする際に使用されるワークキーは、上記暗号化ＥＭＭデータに含まれている暗号化ワークキーでは無く、上記視聴許可システムから供給されたワークキーテーブルから得られる暗号化されていないワークキーであることを特徴とする請求の範囲第１８項に記載のプログラム配信システム。

２０．上記第２の暗号化手段は、

上記視聴許可システムから供給されたワークキーテーブルを参照することによって、上記ＥＣＭデータに含まれるワークキー識別番号からワークキーを得、

上記第２の暗号化手段において、上記ワークキーテーブルから得られたワークキーを使用して上記ＥＣＭデータに含まれるスクランブルキーを暗号化し、

上記第２の暗号化回路において暗号化された暗号化スクランブルキーを、暗号化ＥＣＭデータとして出力することを特徴とすることを特徴とする請求の範囲第１９項に記載のプログラム配信システム。

２１．上記符号化システムから出力される符号化ストリーム、上記視聴許可システムから出力される暗号化ＥＭＭデータ及びＥＣＭデータは、トランスポートストリームパケットの形態で出力され、上記トランスポートストリームパケットのには、トランスポートストリームパケットを識別するためのパケットＩＤが付与されていることを特徴とする請求の範囲第２０項に記載のプログラム配信システム。

２２．上記マルチプレクサシステムは、

上記ＥＣＭデータに含まれるスクランブルキーを暗号化し、上記多重化手段に暗号化ＥＣＭデータとして出力するための第２の暗号化手段をさらに備えたことを特徴とする請求の範囲第２１項に記載のプログラム配信システム。

２３．上記スクランブル手段は、

上記暗号化ＥＭＭデータ及び上記暗号化ＥＣＭデータはスクランブルせずに、上記プログラムを構成する複数のデータエレメントのみをスクランブルすることを特徴とする請求の範囲第２２項に記載のプログラム配信システム。

２４．上記スクランブル手段は、

上記データエレメントを含んだトランスポートストリームパケットのパケットＩＤと上記データエレメントに対してそれぞれ設定されたスクランブルキーとを対応付けたテーブルに基いて、上記データエレメントに対応付けられたスクランブルキーを使用して、上記データエレメントをスクランブルすることを特徴とする請求の範囲第２２項に記載のプログラム配信システム。

２５．上記スクランブル手段は、

上記多重化手段から上記スクランブル手段に供給されたトランスポートストリームパケットの全てのトランスポートストリームパケットのパケットＩＤを検出

し、

上記パケットＩＤと上記スクランブルキーとを対応付けたテーブルに基いて、上記検出されたパケットＩＤに対してスクランブルキーが設定されているか否かを判断し、

上記パケットＩＤに対してスクランブルキーが設定されている場合には、上記パケットＩＤによって示されるトランスポートストリームパケットに含まれるデータエレメントを、設定されたスクランブルキーを使用してスクランブルし、

上記パケットＩＤに対してスクランブルキーが設定されていない場合には、上記パケットＩＤによって示されるトランスポートストリームパケットに含まれるデータはスクランブルしないことを特徴とする請求の範囲第２２項に記載のプログラム配信システム。

２６．上記マルチプレクサシステムは、

上記ＥＣＭデータに含まれるスクランブルキーを暗号化するための第２の暗号化手段と、上記マルチプレクサシステムにトランスポートストリームパケットの形態で供給されたデータをそれぞれバッファリングし、トランスポートストリームパケットの単位の上記多重化手段に出力するバッファ手段をさらに備えたことを特徴とする請求の範囲第２０項に記載のプログラム配信システム。

２７．上記マルチプレクサシステムは、

上記データエレメントを含んだトランスポートストリームパケットをバッファリングするための複数のバッファのバッファ残量を監視し、

上記データエレメントを含んだトランスポートストリームパケットをバッファリングするための複数のバッファのいずれかがオーバーフローしそうなときには、上記ＥＭＭデータを含んだトランスポートストリームパケットをバッファリングするためのバッファからＥＭＭデータを含んだトランスポートストリームパケットを上記多重化手段に出力する代わりに、上記オーバフローしそうなバッファ

から上記データエレメントを含んだトランスポートストリームパケットを上記多重化手段に出力することを特徴とする請求の範囲第２６項に記載のプログラム配信システム。

２８．上記マルチプレクサシステムから出力されたトランスポートストリームを、伝送路を介して受信側に配信する配信システムと、

上記伝送路を介して伝送されたトランスポートストリームを受信する受信システムとをさらに備えていることを特徴とする請求の範囲第２０項に記載のプログラム配信システム。

２９．上記受信システムは、

上記伝送されたトランスポートストリームをデマルチプレクスするデマルチプレクサと、上記スクランブルされた各データエレメントを、供給されたスクランブルキーを使用してそれぞれデスクランブルするデスクランブラーと、

上記デスクランブルされたデータをデータエレメント毎にそれぞれデコードするデコーダと、上記トランスポートストリームを構成するトランスポートストリームパケットを解析するＣＰＵと、上記トランスポートストリームに含まれる暗号化スクランブルキーを解読し、暗号解読されたスクランブルキーを上記デスクランブラーに供給するセキュリティモジュールと、

を備えたことを特徴とする請求の範囲第２８項に記載のプログラム配信システム。

３０．上記セキュリティモジュールは、

上記伝送されたトランスポートストリームに含まれる暗号化ＥＭＭデータに含まれる自己の契約情報を記憶するメモリ手段と、

上記伝送されたトランスポートストリーム中に含まれる暗号化ワークキーと上記顧客管理システムにおいて使用されたマスターキーと同じマスターキーを受取

り、上記マスターキーを使用して上記暗号化ワークキーの暗号を解読する第１の暗号解読手段と、

上記トランスポートストリーム中に含まれる暗号化スクランブルキーと上記第１の暗号解読手段から供給された暗号解読されやワークキーとを受取り、上記暗号解読されたワークキーを使用して上記暗号化スクランブルの暗号を解読する第２の暗号解読手段と、

を備えたことを特徴とする請求の範囲第２９項に記載のプログラム配信システム。

３１．上記ＣＰＵは、

上記デマルチプレクサから供給された暗号化ＥＣＭデータを含んだトランスポートストリームパケットから、受信者が契約しているプログラム又はデータエレメントに関する暗号化ＥＣＭデータを有するトランスポートストリームパケットのみをフィルタリングし、

上記フィルタリングされたトランスポートストリームパケットに含まれる暗号化ＥＣＭデータを解析することによって、上記暗号化ＥＣＭデータから上記暗号化スクランブルキーを得ることを特徴とする請求の範囲第３０項に記載のプログラム配信システム。

３２．上記セキュリティモジュールは、

上記ＣＰＵから上記プログラムに対応付けられた暗号化スクランブルキーが供給された場合には、供給された暗号化スクランブルキーの暗号を解読し、上記プログラムを構成する複数のデータエレメントに対応する複数のデスクランブラーに対して同じスクランブルキーをそれぞれ供給し、

上記ＣＰＵから上記複数のデータエレメントにそれぞれ対応付けられた複数の暗号化スクランブルキーが供給された場合には、供給された複数の暗号化スクランブルキーの暗号をそれぞれ解読し、上記複数のデータエレメントのうち契約し

ているデータエレメントに対応する複数のデスクランブラーに対して、それぞれ異なるスクランブルキーを供給することを特徴とする請求の範囲３１項に記載のプログラム配信システム。

３３．上記視聴許可システムは、

上記スクランブルキーを暗号化するために使用されるワークキーをマスターキーを使用して暗号化するための第１の暗号化手段を備え、

上記第１の暗号化手段によって暗号化された暗号化ワークキーと上記顧客を識別するための顧客識別番号とを、暗号化ＥＭＭデータとして上記マルチプレクサシステムに供給し、

上記暗号化手段において暗号化されたワークキーを識別するためのワークキー識別番号と上記スクランブルキーとを、ＥＣＭデータとして上記マルチプレクサシステムに供給する

ことを特徴とする請求の範囲第１２項に記載のプログラム配信システム。

３４．上記複数のプログラム、上記プログラムを構成する複数のデータエレメント、上記複数のＥＣＭデータ及び上記複数のＥＭＭデータをどのように多重化するかを示すプログラム仕様情報を生成し、この生成されたプログラム使用情報に対応するように、上記複数のプログラム、上記複数のデータエレメント、上記複数のＥＣＭデータ及び上記複数のＥＭＭデータを多重化するように上記エンコーダシステム及び上記マルチプレクサシステムを制御する、エンコーダ／マルチプレクサコントロールシステムを備えたことを特徴とする請求の範囲第３３項に記載のプログラム配信システム。

３５．上記データ配信システムから出力されるトランスポートストリーム内において、上記記プログラムを構成する複数のデータエレメントが含まれるトランスポートストリームパケット、上記ＥＣＭデータが含まれるトランスポートストリ

ームパケット及び上記ＥＭＭデータが含まれるトタランスポートストリームパケットのパケットＩＤを識別するためのプログラム仕様情報を生成し、

このプログラム使用情報に対応するように、上記記プログラムを構成する複数のデータエレメントが含まれるトランスポートストリームパケット、上記ＥＣＭデータが含まれるトランスポートストリームパケット及び上記ＥＭＭデータが含まれるトタランスポートストリームパケットを多重化するように、上記エンコーダシステム及び上記マルチプレクサシステムを制御するエンコーダ／マルチプレクサコントロールシステムを備えたことを特徴とする請求の範囲第３３項に記載のプログラム配信システム。

３６．上記エンコーダシステムは、上記各符号化されたデータエレメンをそれぞれトランスポートストリームパケットの形態を有したエレメンタリパケットとして上記マルチプレクサシステムに供給し、上記視聴許可システムは、上記暗号化ＥＭＭデータ及び上記ＥＣＭデータを、それぞれ、トランスポートストリームパケットの形態を有した暗号化ＥＭＭパケット及びＥＣＭパケットとして上記マルチプレクサシステムに供給し、

上記エンコーダ／マルチプレクサコントロールシステムは、上記プログラム仕様情報を、トランスポートストリームパケットの形態を有したＰＳＩパケットとして上記マルチプレクサシステムに供給することを特徴とする請求の範囲第３４項に記載のプログラム配信システム。

３７．上記マルチプレクサシステムは、

上記多重化手段の前段に、上記ＥＣＭデータに含まれるスクランブルキーを暗号化するための第２の暗号化手段をさらに備えたことを特徴とする請求の範囲第３６項に記載のプログラム配信システム。

３８．上記視聴許可システムは、

上記ワークキーと、該ワークキーを識別するためのワークキー識別番号とをそれぞれ対応付けたワークキーテーブルを上記マルチプレクサシステムの上記第２の暗号化手段に供給することを特徴とする請求の範囲第３７項に記載のプログラム配信システム。

３９．上記第２の暗号化手段は、

上記ＥＣＭデータに含まれるワークキー識別番号から、上記ワークキーテーブルを参照することによってワークキーを得、

上記第２の暗号化手段において、上記ワークキーテーブルから得られたワークキーを使用して上記ＥＣＭデータに含まれるスクランブルキーを暗号化し、

上記第２の暗号化回路において暗号化された暗号化スクランブルキーを、暗号化ＥＣＭデータとして上記多重化手段に供給することを特徴とする請求の範囲第３８項に記載のプログラム配信システム。

４０．上記エンコーダ／マルチプレクサコントロールシステムは、

上記マルチプレクサシステムにトランスポートストリームパケットの形態として供給される全てのトランスポートストリームパケットに対して、上記トランスポートストリームパケットを識別するためのパケットＩＤを付与することを特徴とする請求の範囲第３９項に記載のプログラム配信システム。

４１．上記プログラム仕様情報は、

少なくとも、プログラムアソシエーションテーブルと、プログラムマップテーブルと、コンディショナルアクセステーブルとから構成されていることを特徴とする請求の範囲第４０項に記載のプログラム配信システム。

４２．上記エンコーダ／マルチプレクサコントロールシステムは、

上記プログラムアソシエーションテーブルを含んだトランスポートストリーム

パケットをＰＡＴパケットとして上記マルチプレクサシステムに供給し、

上記プログラムマップテーブルを含んだトランスポートストリームパケットをＰＭＴパケットとして上記マルチプレクサシステムに供給し、

上記コンディショナルアクセステーブルを含んだトランスポートストリームパケットをＣＡＴパケットとして上記マルチプレクサシステムに供給することを特徴とする請求の範囲第４１項に記載のプログラム配信システム。

４３．上記プログラムアソシエーションテーブルは、プログラム番号とそのプログラム番号に対応するＰＭＴパケットのパケットＩＤを指定するためのテーブルであって、

上記プログラムマップテーブルは、プログラムを構成する複数のデータエレメントが含まれるトランスポートストリームパケットのパケットＩＤをそれぞれ指定するためのテーブルであって、上記コンディショナルアクセステーブルは、上記暗号化ＥＭＭパケットのパケットＩＤを指定するためのテーブルであることを特徴とする請求の範囲第４２項に記載のプログラム配信システム。

４４．上記プログラムアソシエーションテーブルには、

プログラムを示すプログラム番号と該プログラムに関連付けられたＰＭＴパケットのパケットＩＤとが記述され、

上記プログラムマップテーブルには、

上記プログラムを示すプログラム番号と、上記プログラムを構成する複数のデータエレメントが含まれるトランスポートストリームパケットが含まれる複数のパケットＩＤと、上記プログラム又は上記データエレメントと関連付けられた暗号化ＥＣＭパケットのパケットＩＤを指定するためのディスクリプタとが記述されている

ことを特徴とする請求の範囲第４３項に記載のプログラム配信システム。

４５．上記プログラムマップテーブル中の上記ディスクリプタが、上記プログラ

ム番号と対応つけられた位置に記述されている場合には、上記ディスクリプタは、上記プログラムを構成する複数のデータエレメントの全てのデータエレメントをスクランブルするためのスクランブルキーを含んだＥＣＭパケットのパケットＩＤを指定し、

上記プログラムマップテーブル中の上記ディスクリプタが、上記プログラムの各データエレメントと対応付けられた位置にそれぞれ記述されている場合には、上記プログラムを構成する複数のデータエレメントの各データエレメントをそれぞれスクランブルするための複数のスクランブルキーを含んだ複数のＥＣＭパケットのパケットＩＤを指定することを特徴とする請求の範囲第４４項に記載のプログラム配信システム。

４６．上記プログラムが、第１のデータエレメントから第ｎのデータエレメントを有し、上記第１のデータエレメントから第ｎのデータエレメントに対して同じスクランブルキーが指定されている場合には、上記プログラムマップテーブルにおいて、

上記プロブラムを示すプルグラム番号と、上記第１番めのデータエレメントから上記第ｎのデータエレメントをそれぞれスクランブルするスクランブルキーを含んだＥＣＭパケットのパケットＩＤとが対応付けられて記述されていることを特徴とする請求の範囲第４５項に記載のプログラム配信システム。

４７．上記プログラムが、第１のデータエレメントから第ｎのデータエレメントを有し、上記第１のデータエレメントから第ｎのデータエレメントに対して少なくとも１つの異なるスクランブルキーが指定されている場合には、

上記プログラムマップテーブルにおいて、

第１番めのデータエレメントが含まれるトランスポートストリームパケットのパケットＩＤと、上記第１番めのデータエレメントをスクランブルするスクランブルキーを含んだＥＣＭデータを含んだトランスポートストリームパケットのパ

ケットＩＤとが対応付けられて記述され、

第ｎ番めのデータエレメントが含まれるトランスポートストリームパケットのパケットＩＤと、上記第ｎ番めのデータエレメントをスクランブルするスクランブルキーを含んだＥＣＭデータを含んだトランスポートストリームパケットのパケットＩＤとが対応付けられて記述されていることを特徴とする請求の範囲第４５項に記載のプログラム配信システム。

４８．上記エンコーダ／マルチプレクサコントロールシステムは、

上記プログラムマップテーブル及び上記コンディショナルアクセステーブルに対して、固有のパケットＩＤを指定することを特徴とする請求の範囲第４２項に記載のプログラム配信システム。

４９．上記スクランブル手段は、

上記プログラム仕様情報、上記ＥＭＭデータ及び上記ＥＣＭデータはスクランブルせずに、上記データエレメントのみをスクランブルすることを特徴とする請求の範囲第４２項に記載のプログラム配信システム。

５０．上記スクランブル手段は、

上記データエレメントを含んだトランスポートストリームパケットのパケットＩＤと上記データエレメントに対して指定されたスクランブルキーとを対応付けた対応テーブルに基いて、上記データエレメントに対して指定されたスクランブルキーを使用して、上記データエレメントをそれぞれスクランブルすることを特徴とする請求の範囲第４２項に記載のプログラム配信システム。

５１．エンコーダ／マルチプレクサコントロールシステムは、

上記ＥＣＭパケット、上記ＥＭＭパケット、上記ＰＳＩパケット、上記エレメンタリーパケットをそれぞれ識別するためのパケットＩＤを指定する際に、各ト

ランスポートストリームパケットに対して割り当てるパケットＩＤが重複しないように過去の処理において使用したパケットＩＤを記憶することを特徴とする請求の範囲第４２項に記載のプログラム配信システム。

５２．エンコーダ／マルチプレクサコントロールシステムは、

各トランスポートストリームパケットに対して割り当てられたパケットＩＤと、該トランスポートストリームパケットに含まれるデータをスクランブルする際に使用するスクランブルキーとを対応付けたテーブルを生成し、

上記パケットＩＤと上記スクランブルキーとを対応付けたテーブルを、上記マルチプレクサシステムに供給することを特徴とする請求の範囲第４２項に記載のプログラム配信システム。

５３．上記スクランブル手段は、

上記パケットＩＤと上記スクランブルキーとを対応付けたテーブルを参照することによって、上記プログラム仕様情報、上記ＥＭＭデータ及び上記ＥＣＭデータはスクランブルせずに、上記データエレメントのみをスクランブルすることを特徴とする請求の範囲第５２項に記載のプログラム配信システム。

５４．上記スクランブル手段は、

上記パケットＩＤと上記スクランブルキーとを対応付けたテーブルを参照することによって、上記データエレメントに対して指定されたスクランブルキーを使用して、上記データエレメントをそれぞれスクランブルすることを特徴とする請求の範囲第５２項に記載のプログラム配信システム。

５５．上記スクランブル手段は、

上記多重化手段から上記スクランブル手段に供給されたトランスポートストリームパケットの全てのトランスポートストリームパケットのパケットＩＤを検出

し、

上記パケットＩＤと上記スクランブルキーとを対応付けたテーブルに基いて、上記検出されたパケットＩＤに対してスクランブルキーが設定されているか否かを判断し、

上記パケットＩＤに対してスクランブルキーが設定されている場合には、上記パケットＩＤによって示されるトランスポートストリームパケットに含まれるデータエレメントを、設定されたスクランブルキーを使用してスクランブルし、

上記パケットＩＤに対してスクランブルキーが設定されていない場合には、上記パケットＩＤによって示されるトランスポートストリームパケットに含まれるデータはスクランブルしないことを特徴とする請求の範囲第５２項に記載のプログラム配信システム。

５６．上記マルチプレクサシステムは、

上記スクランブルキーを暗号化する第２の暗号化手段と、

上記ＰＡＴパケット、上記ＰＭＴパケット、上記ＣＡＴパケット、上記データエレメントを含んだトランスポートストリームパケット、上記暗号化ＥＭＭパケット及び上記暗号化ＥＣＭパケットをそれぞれバッファリングし、上記多重化手段に対してトランスポートストリームパケットの単位で出力するための複数のバッファ手段とをさらに備えたことを特徴とする請求の範囲第３６項に記載のプログラム配信システム。

５７．上記マルチプレクサシステムは、

上記データエレメントを含んだトランスポートストリームパケットをバッファリングするための複数のバッファのバッファ残量を監視し、

上記データエレメントを含んだトランスポートストリームパケットをバッファリングするための複数のバッファのいずれかがオーバーフローしそうなときには、上記ＥＭＭパケットをバッファリングするためのバッファからＥＭＭパケット

を上記多重か手段に出力する代わりに、上記オーバフローしそうなバッファから上記データエレメントを含んだトランスポートストリームパケットを上記多重化手段に出力することを特徴とする請求の範囲第５６項に記載のプログラム配信システム。

５８．上記マルチプレクサシステムから出力されたトランスポートストリームを、伝送路を介して受信側に配信する配信システムと、

上記伝送路を介して伝送されたトランスポートストリームを受信する受信システムとをさらに備えていることを特徴とする請求の範囲４７項に記載のプログラム配信システム。

５９．上記受信システムは、

上記伝送されたトランスポートストリームをデマルチプレクスするデマルチプレクサと、上記スクランブルされた各データエレメントを、供給されたスクランブルキーを使用してそれぞれデスクランブルするデスクランブラーと、

上記デスクランブルされたデータをデータエレメント毎にそれぞれデコードするデコーダと、上記トランスポートストリームを構成するトランスポートストリームパケットを解析するＣＰＵと、上記トランスポートストリームに含まれる暗号化スクランブルキーを解読し、暗号解読されたスクランブルキーを上記デスクランブラーに供給するセキュリティモジュールと、

を備えたことを特徴とする請求の範囲第５８項に記載のプログラム配信システム。

６０．上記ＣＰＵは、

上記トランスポートストリームに含まれるプログラムアソシエーションテーブルを解析するＰＡＴ解析手段と、

上記トランスポートストリームに含まれるプログラムマップテーブルを解析す

るＰＭＴ解析手段と、上記トランスポートストリームに含まれるコンディショナルアクセステーブルを解析するＣＡＴ解析手段と、

上記トランスポートストリームに含まれる暗号化ＥＭＭデータを解析するＥＭＭ解析手段と、上記トランスポートストリームに含まれる暗号化ＥＣＭデータを解析するＥＣＭ解析手段とを備えていることを特徴とする請求の範囲第５９項に記載のプログラム配信システム。

６１．上記セキュリティモジュールは、

上記ＥＭＭデータに含まれる自己の契約情報を記憶するメモリ手段と、

上記トランスポートストリーム中に含まれる暗号化ワークキーと上記顧客管理システムにおいて使用されたマスターキーと同じマスターキーを受取り、上記マスターキーを使用して上記暗号化ワークキーの暗号を解読する第１の暗号解読手段と、

上記トランスポートストリーム中に含まれる暗号化スクランブルキーと上記第１の暗号解読手段から供給された暗号解読されやワークキーとを受取り、上記暗号解読されたワークキーを使用して上記暗号化スクランブルの暗号を解読する第２の暗号解読手段と、

を備えたことを特徴とする請求の範囲第５９項に記載のプログラム配信システム。

６２．上記ＣＰＵは、

上記トランスポートストリームに含まれるプログラムアソシエーションテーブル及びプログラムマップテーブルを解析することによって、上記プログラムを構成する各データエレメントを含んだトランスポートストリームパケットを識別し、上記データエレメントを含んだトランスポートストリームパケットを適切な上記スクランブラーにそれぞれ出力するように上記デマルチプレクサを制御する請求の範囲第６１項に記載のプログラム配信システム。

６３．上記ＣＰＵは、

上記トランスポートストリームに含まれるコンディショナルアクセステーブルを解析することによって、ＥＭＭデータが含まれるトランスポートストリームパケットを検出し、

上記ＥＭＭデータが含まれるトランスポートストリームから、受信者が契約しているプログラムに関するＥＭＭデータを有するトランスポートストリームパケットのみをフィルタリングし、上記フィルタリングされたトランスポートストリームパケットに含まれるＥＭＭデータを解析することによって、ＥＭＭデータから上記暗号化ワークキーを得ることを特徴とする請求の範囲第６２項に記載のプログラム配信システム。

６４．上記ＣＰＵは、

上記トランスポートストリームに含まれるプログラムアソシエーションテーブル及びこのプログラムアソシエーションテーブルによって指定されたプログラムマップテーブルを解析することによって、上記プログラムを構成する複数のデータエレメント及び上記ＥＣＭデータを含んだトランスポートストリームパケットをそれぞれ検出し、

上記複数のデータエレメントを含んだトランスポートストリームパケットをそれぞれ上記デスクランブラーに供給すると共に、上記ＥＣＭデータを含んだトランスポートストリームパケットを受け取るように、上記デマルチプレクサを制御することを特徴とする請求の範囲第６１項に記載のプログラム配信システム。

６５．上記ＣＰＵは、

上記デマルチプレクサから供給された暗号化ＥＣＭデータを含んだトランスポートストリームパケットから、受信者が契約しているプログラム又はデータエレメントに関する暗号化ＥＣＭデータを有するトランスポートストリームパケット

のみをフィルタリングし、

上記フィルタリングされたトランスポートストリームパケットに含まれる暗号化ＥＣＭデータを解析することによって、上記暗号化ＥＣＭデータから上記暗号化スクランブルキーを得ることを特徴とする請求の範囲第６４項に記載のプログラム配信システム。

６６．上記プログラムマップテーブルのシンタックスにおいて、上記プログラム番号と上記暗号化ＥＣＭパケットのパケットＩＤとが対応付けられて記述されている場合には、

上記ＣＰＵは、上記パケットＩＤによって指定された暗号化ＥＣＭパケットに含まれている暗号化スクランブルキーを、上記プログラムに対応する暗号化スクランブルキーとして上記セキュリティモジュールに供給し、

上記プログラムマップテーブルのシンタックスにおいて、上記プログラムを構成する複数のデータエレメントと上記複数の暗号化ＥＣＭパケットのパケットＩＤとがそれぞれ対応付けられて記述されている場合には、

上記ＣＰＵは、上記複数のパケットＩＤによって指定された暗号化ＥＣＭパケットに含まれるそれぞれ異なる複数のスクランブルキーを、上記複数のデータエレメントに対応する暗号化スクランブルキーとして上記セキュリティモジュールに供給する

ことを特徴とする請求の範囲６５項に記載のプログラム配信システム。

６７．上記セキュリティモジュールは、

上記ＣＰＵから上記プログラムに対応する暗号化スクランブルキーが供給された場合には、供給された暗号化スクランブルキーの暗号を解読し、上記プログラムを構成する複数のデータエレメントに対応する複数のデスクランブラーに対して同じスクランブルキーをそれぞれ供給し、

上記ＣＰＵから上記複数のデータエレメントにそれぞれ対応する複数の暗号化

スクランブルキーが供給された場合には、供給された複数の暗号化スクランブルキーの暗号をそれぞれ解読し、上記複数のデータエレメントのうち契約しているデータエレメントに対応する複数のデスクランブラーに対して、それぞれ異なるスクランブルキーを供給する請求の範囲第６６項に記載のプログラム配信システム。

６８．複数のデータエレメントから構成されるプログラムを伝送するプログラム伝送システムにおいて、顧客が契約したプログラム及びデータエレメントのみを視聴できるように、上記プログラムに含まれる複数のデータエレメントをスクランブルする際に使用される複数のスクランブルキーを生成する視聴許可システムと、

上記複数のプログラムに含まれるデータエレメントをそれぞれ符号化し、その符号化データエレメントから構成される符号化ストリームを上記各プログラム毎に生成する符号化システムと、上記符号化手段から各プログラム毎に出力された符号化ストリームを多重化する多重化手段と、上記視聴許可システムにおいて生成されたスクランブルキーに基いて、上記多重化ストリームに含まれる符号化データエレメントに対して各データエレメント毎に選択的にスクランブルをかけるスクランブル手段とを備えたマルチプレクサシステムと、

上記マルチプレクサシステムにおいてマルチプレクサされたストリームを伝送する伝送システムを備えたことを特徴とするプログラム伝送システム。

６９．複数のデータエレメントをそれぞれ有した複数のプログラムを伝送するプログラム伝送システムにおいて、

上記データエレメント毎にスクランブルキーを生成するスクランブルキー生成手段と、上記複数のプログラムに含まれるデータエレメントをそれぞれ符号化し、その符号化データエレメントから構成される符号化ストリームを上記各プログラム毎に生成する符号化手段と、

上記符号化手段から各プログラム毎に出力された符号化ストリームを多重化し、多重化ストリームを生成する多重化手段と、

上記スクランブルキー生成手段によって生成されたスクランブルキーに基いて、上記多重化ストリームに含まれる符号化データエレメントに対して各データエレメント毎にスクランブルをかけるスクランブル手段と上記スクランブルがかけられた多重化ストリームを伝送する伝送手段と

を備えたことを特徴とするプログラム伝送システム。

７０．複数のデータエレメントから構成されるプログラムを放送する有料放送システムにおいて、顧客のデータエレメント単位の契約を管理するシステムであって、上記顧客に対して契約したデータエレメントに基いて課金処理を行なう顧客管理システムと、

顧客が契約したデータエレメントのみを視聴できるように、上記データエレメント単位に上記データエレメントをスクランブルするために使用される複数のスクランブルキーを生成する視聴許可システムと、上記複数のプログラムに含まれるデータエレメントをそれぞれ符号化し、その符号化データエレメントから構成される符号化ストリームを上記各プログラム毎に生成する符号化システムと、上記符号化手段から各プログラム毎に出力された符号化ストリームを多重化する多重化手段と、上記視聴許可システムにおいて生成された複数のスクランブルキーに基いて、上記多重化ストリームに含まれる符号化データエレメントに対して各データエレメント毎に選択的にスクランブルをかけるスクランブル手段とを備えたマルチプレクサシステムと、

を備えたことを特徴とする有料放送システム。

７１．複数のデータエレメントから構成されるプログラムを伝送するプログラム伝送方法において、上記顧客が契約したプログラム及びデータエレメントのみを視聴できるように、上記プログラムに含まれる複数のデータエレメントをスクラ

ンブルする際に使用される複数のスクランブルキーを生成するスクランブルキー生成工程と、

上記複数のプログラムに含まれるデータエレメントをそれぞれ符号化し、その符号化データエレメントから構成される符号化ストリームを上記各プログラム毎に生成する符号化工程と、

上記符号化手段から各プログラム毎に出力された複数の符号化ストリームを多重化する多重化工程と、上記生成されたスクランブルキーに基いて、上記多重化ストリームに含まれる符号化データエレメントに対して各データエレメント毎に選択的にスクランブルをかけるスクランブル工程と、を備えたことを特徴とするプログラム伝送方法。

７２．上記スクランブルキー生成工程において、

上記スクランブルキーを暗号化するために使用されるワークキーをマスターキーを使用して暗号化し、上記暗号化された暗号化ワークキーと上記顧客を識別するための顧客識別番号とを、暗号化ＥＭＭデータとして出力すると共に、

上記暗号化されたワークキーを識別するためのワークキー識別番号と上記スクランブルキーとを、ＥＣＭデータとして出力する

ことを特徴とする請求の範囲第７１項に記載のプログラム伝送方法。

７３．上記複数のプログラム、上記プログラムを構成する複数のデータエレメント、上記複数のＥＣＭデータ及び上記複数のＥＭＭデータをどのように多重化するかを示すプログラム仕様情報を生成するプログラム仕様情報生成工程をさらに備え、

上記多重化工程において、この生成されたプログラム使用情報に対応するように、上記複数のプログラム、上記複数のデータエレメント、上記複数のＥＣＭデータ及び上記複数のＥＭＭデータを多重化することを特徴とする請求の範囲第７２項に記載のプログラム伝送方法。

７４．上記スクランブルキー生成工程において、上記暗号化ＥＭＭデータ及び上記ＥＣＭデータを、それぞれ、トランスポートストリームパケットの形態を有した暗号化ＥＭＭパケット及びＥＣＭパケットとして出力し、

上記符号化工程において、上記各符号化されたデータエレメンをトランスポートストリームパケットの形態を有したエレメンタリパケットとして出力し、

上記プログラム仕様情報生成工程において、上記プログラム仕様情報を、トランスポートストリームパケットの形態を有したＰＳＩパケットとして出力することを特徴とする請求の範囲第７３項に記載のプログラム伝送方法。

７５．上記多重化工程において、上記ＥＣＭデータに含まれるスクランブルキーを暗号化する暗号化工程を有することを特徴とする請求の範囲第７４項に記載のプログラム伝送方法。

７６．上記スクランブルキー生成工程において、

上記ワークキーと、該ワークキーを識別するためのワークキー識別番号とをそれぞれ対応付けたワークキーテーブルを生成することを特徴とする請求の範囲第７５項に記載のプログラム伝送方法。

７７．上記多重化工程の上記暗号化工程において、

上記ＥＣＭデータに含まれるワークキー識別番号から、上記ワークキーテーブルを参照することによってワークキーを得、

上記ワークキーテーブルから得られたワークキーを使用して上記ＥＣＭデータに含まれるスクランブルキーを暗号化し、

上記第２の暗号化回路において暗号化された暗号化スクランブルキーを、暗号化ＥＣＭデータとして出力することを特徴とする請求の範囲第７６項に記載のプログラム伝送方法。

７８．上記プログラム仕様情報生成工程において、

上記マルチプレクサシステムにトランスポートストリームパケットの形態として供給される全てのトランスポートストリームパケットに対して、上記トランスポートストリームパケットを識別するためのパケットＩＤを付与することを特徴とする請求の範囲第７７項に記載のプログラム伝送方法。

７９．上記プログラム仕様情報は、

少なくとも、プログラムアソシエーションテーブルと、プログラムマップテーブルと、コンディショナルアクセステーブルとから構成されていることを特徴とする請求の範囲第７８項に記載のプログラム伝送方法。

８０．上記プログラム仕様情報生成工程において、

上記プログラムアソシエーションテーブルを含んだトランスポートストリームパケットをＰＡＴパケットとして上記マルチプレクサシステムに供給し、

上記プログラムマップテーブルを含んだトランスポートストリームパケットをＰＭＴパケットとして上記マルチプレクサシステムに供給し、

上記コンディショナルアクセステーブルを含んだトランスポートストリームパケットをＣＡＴパケットとして上記マルチプレクサシステムに供給することを特徴とする請求の範囲第７９項に記載のプログラム伝送方法。

８１．上記プログラムアソシエーションテーブルは、プログラム番号とそのプログラム番号に対応するＰＭＴパケットのパケットＩＤを指定するためのテーブルであって、

上記プログラムマップテーブルは、プログラムを構成する複数のデータエレメントが含まれるトランスポートストリームパケットのパケットＩＤをそれぞれ指定するためのテーブルであって、上記コンディショナルアクセステーブルは、上記暗号化ＥＭＭパケットのパケットＩＤを指定するためのテーブルであることを

特徴とする請求の範囲第８０項に記載のプログラム伝送方法。

８２．上記プログラムアソシエーションテーブルには、

プログラムを示すプログラム番号と該プログラムに関連付けられたＰＭＴパケットのパケットＩＤとが記述され、

上記プログラムマップテーブルには、

上記プログラムを示すプログラム番号と、上記プログラムを構成する複数のデータエレメントが含まれるトランスポートストリームパケットが含まれる複数のパケットＩＤと、上記プログラム又は上記データエレメントと関連付けられた暗号化ＥＣＭパケットのパケットＩＤを指定するためのディスクリプタとが記述されている

ことを特徴とする請求の範囲第８１項に記載のプログラム伝送方法。

８３．上記プログラムマップテーブル中の上記ディスクリプタが、上記プログラム番号と対応つけられた位置に記述されている場合には、上記ディスクリプタは、上記プログラムを構成する複数のデータエレメントの全てのデータエレメントをスクランブルするためのスクランブルキーを含んだＥＣＭパケットのパケットＩＤを指定し、

上記プログラムマップテーブル中の上記ディスクリプタが、上記プログラムの各データエレメントと対応付けられた位置にそれぞれ記述されている場合には、上記プログラムを構成する複数のデータエレメントの各データエレメントをそれぞれスクランブルするための複数のスクランブルキーを含んだ複数のＥＣＭパケットのパケットＩＤを指定することを特徴とする請求の範囲第８２項に記載のプログラム伝送方法。

８４．上記プログラムが、第１のデータエレメントから第ｎのデータエレメントを有し、上記第１のデータエレメントから第ｎのデータエレメントに対して少な

くとも１つの異なるスクランブルキーが指定されている場合には、

上記プログラムマップテーブルにおいて、

第１番めのデータエレメントが含まれるトランスポートストリームパケットのパケットＩＤと、上記第１番めのデータエレメントをスクランブルするスクランブルキーを含んだＥＣＭデータを含んだトランスポートストリームパケットのパケットＩＤとが対応付けられて記述され、

第ｎ番めのデータエレメントが含まれるトランスポートストリームパケットのパケットＩＤと、上記第ｎ番めのデータエレメントをスクランブルするスクランブルキーを含んだＥＣＭデータを含んだトランスポートストリームパケットのパケットＩＤとが対応付けられて記述されていることを特徴とする請求の範囲第８３項に記載のプログラム伝送方法。

８５．上記スクランブル工程において、

上記データエレメントを含んだトランスポートストリームパケットのパケットＩＤと上記データエレメントに対して指定されたスクランブルキーとを対応付けた対応テーブルに基いて、上記データエレメントに対して指定されたスクランブルキーを使用して、上記プログラム仕様情報、上記ＥＭＭデータ及び上記ＥＣＭデータはスクランブルせずに、上記データエレメントのみをそれぞれスクランブルすることを特徴とする請求の範囲第８０項に記載のプログラム伝送方法。

８６．上記プログラム仕様情報生成工程において、

各トランスポートストリームパケットに対して割り当てられたパケットＩＤと、該トランスポートストリームパケットに含まれるデータをスクランブルする際に使用するスクランブルキーとを対応付けたテーブルを生成し、

上記パケットＩＤと上記スクランブルキーとを対応付けたテーブルを、上記マルチプレクサシステムに供給することを特徴とする請求の範囲第８０項に記載のプログラム伝送方法。

８７．上記スクランブル手段は、

上記パケットＩＤと上記スクランブルキーとを対応付けたテーブルを参照することによって、上記プログラム仕様情報、上記ＥＭＭデータ及び上記ＥＣＭデータはスクランブルせずに、上記データエレメントのみをスクランブルすることを特徴とする請求の範囲第８６項に記載のプログラム伝送方法。

８８．上記スクランブル工程において、

上記多重化手段から上記スクランブル手段に供給されたトランスポートストリームパケットの全てのトランスポートストリームパケットのパケットＩＤを検出し、

上記パケットＩＤと上記スクランブルキーとを対応付けたテーブルに基いて、上記検出されたパケットＩＤに対してスクランブルキーが設定されているか否かを判断し、

上記パケットＩＤに対してスクランブルキーが設定されている場合には、上記パケットＩＤによって示されるトランスポートストリームパケットに含まれるデータエレメントを、設定されたスクランブルキーを使用してスクランブルし、

上記パケットＩＤに対してスクランブルキーが設定されていない場合には、上記パケットＩＤによって示されるトランスポートストリームパケットに含まれるデータはスクランブルしないことを特徴とする請求の範囲第８６項に記載のプログラム伝送方法。

８９．上記多重化工程において、

上記スクランブルキーを上記ワークキーを仕様して暗号化し、

上記ＰＡＴパケット、上記ＰＭＴパケット、上記ＣＡＴパケット、上記データエレメントを含んだトランスポートストリームパケット、上記暗号化ＥＭＭパケット及び上記暗号化ＥＣＭパケットをそれぞれ複数のバッファ手段にバッファリ

ングすることを特徴とする請求の範囲第７４項に記載のプログラム伝送方法。

９０．上記多重化工程において、

上記データエレメントを含んだトランスポートストリームパケットをバッファリングするための複数のバッファのバッファ残量を監視し、

上記データエレメントを含んだトランスポートストリームパケットをバッファリングするための複数のバッファのいずれかがオーバーフローしそうなときには、上記ＥＭＭパケットをバッファリングするためのバッファからＥＭＭパケットを上記多重か手段に出力する代わりに、上記オーバフローしそうなバッファから上記データエレメントを含んだトランスポートストリームパケットを出力することを特徴とする請求の範囲第８９項に記載のプログラム伝送方法。

９１．プログラム配信システムから配信された複数のプログラム及び上記プログラムを構成する複数のデータエレメントのうち、契約されたプログラム及びデータエレメントのみを限定的に受信する限定受信システムにおいて、

上記トランスポートストリームから、上記プログラムを構成する複数のスクランブルされたデータエレメントを含んでいるトランスポートストリームパケットをデマルチプレクスすると共に、上記複数のデータエレメントに対応付けられた複数の暗号化スクランブルキーを含んだ複数のトランスポートストリームパケットをデマルチプレクスするデマルチプレクサ手段と、

上記デマルチプレクスされた複数の暗号化スクランブルキーを含んだ複数のトランスポートストリームパケットから、受信者が契約したプログラム及びデータエレメントに関連付けられた暗号化スクランブルキーを含んだトランスポートストリームパケットをフィルタリングするフィルタ手段と、上記フィルタリングされた複数のトランスポートストリームパケットに含まれる複数の暗号化スクランブルキーの暗号を解読し、暗号解読された複数のスクランブルキーを生成する暗号解読手段と、上記複数のデータエレメントに対応付けられた複数の暗号解読さ

れたスクランブルキーを使用して、上記デマルチプレクサされた複数のデータエレメントを上記データエレメント毎にデスクランブルするデスクランブル手段と、

上記デスクランブル手段においてデスクランブルされた複数のデータエレメントをそれぞれデコードするデコード手段と

から構成されることを特徴とする限定受信システム。

９２．上記プログラム配信システムは、

顧客のプログラム毎及びデータエレメント毎の契約を管理するための顧客管理システムと、上記顧客が契約したプログラム及びデータエレメントのみを視聴できるように、上記プログラムに含まれる複数のデータエレメントをスクランブルする際に使用される複数のスクランブルキーを生成する視聴許可システムと、

上記複数のプログラムに含まれるデータエレメントをそれぞれ符号化し、その符号化データエレメントから構成される符号化ストリームを上記各プログラム毎に生成する符号化システムと、上記符号化手段から各プログラム毎に出力された符号化ストリームを多重化する多重化手段と、上記視聴許可システムにおいて生成されたスクランブルキーに基いて、上記多重化ストリームに含まれる符号化データエレメントに対して各データエレメント毎に選択的にスクランブルをかけるスクランブル手段とを備えたマルチプレクサシステムと、

上記マルチプレクサシステムにおいてマルチプレクサされたストリームを伝送する伝送システムを備えたことを特徴とする請求の範囲第９１項に記載の限定受信システム。

９３．上記視聴許可システムは、

上記スクランブルキーを暗号化するために使用されるワークキーをマスターキーを使用して暗号化するための第１の暗号化手段を備え、

上記第１の暗号化手段によって暗号化された暗号化ワークキーと上記顧客を識

別するための顧客識別番号とを、暗号化ＥＭＭデータとして上記マルチプレクサシステムに供給し、

上記暗号化手段において暗号化されたワークキーを識別するためのワークキー識別番号と上記スクランブルキーとを、ＥＣＭデータとして上記マルチプレクサシステムに供給する

ことを特徴とする請求の範囲第９２項に記載の限定受信システム。

９４．上記複数のプログラム、上記プログラムを構成する複数のデータエレメント、上記複数のＥＣＭデータ及び上記複数のＥＭＭデータをどのように多重化するかを示すプログラム仕様情報を生成し、この生成されたプログラム使用情報に対応するように、上記複数のプログラム、上記複数のデータエレメント、上記複数のＥＣＭデータ及び上記複数のＥＭＭデータを多重化するように上記エンコーダシステム及び上記マルチプレクサシステムを制御する、エンコーダ／マルチプレクサコントロールシステムを備えたことを特徴とする請求の範囲第９３項に記載の限定受信システム。

９５．上記エンコーダシステムは、上記各符号化されたデータエレメントをそれぞれトランスポートストリームパケットの形態を有したエレメンタリパケットとして上記マルチプレクサシステムに供給し、上記視聴許可システムは、上記暗号化ＥＭＭデータ及び上記ＥＣＭデータを、それぞれ、トランスポートストリームパケットの形態を有した暗号化ＥＭＭパケット及びＥＣＭパケットとして上記マルチプレクサシステムに供給し、

上記エンコーダ／マルチプレクサコントロールシステムは、上記プログラム仕様情報を、トランスポートストリームパケットの形態を有したＰＳＩパケットとして上記マルチプレクサシステムに供給することを特徴とする請求の範囲第９４項に記載の限定受信システム。

９６．上記マルチプレクサシステムは、

上記ＥＣＭデータに含まれるスクランブルキーを暗号化するための第２の暗号化手段をさらに備えたことを特徴とする請求の範囲第９５項に記載の限定受信システム。

９７．上記視聴許可システムは、

上記ワークキーと、該ワークキーを識別するためのワークキー識別番号とをそれぞれ対応付けたワークキーテーブルを上記マルチプレクサシステムの上記第２の暗号化手段に供給することを特徴とする請求の範囲第９６項に記載の限定受信システム。

９８．上記第２の暗号化手段は、

上記ＥＣＭデータに含まれるワークキー識別番号から、上記ワークキーテーブルを参照することによってワークキーを得、

上記第２の暗号化手段において、上記ワークキーテーブルから得られたワークキーを使用して上記ＥＣＭデータに含まれるスクランブルキーを暗号化し、

上記第２の暗号化回路において暗号化された暗号化スクランブルキーを、暗号化ＥＣＭデータとして上記多重化手段に供給することを特徴とする請求の範囲第９７項に記載の限定受信システム。

９９．上記エンコーダ／マルチプレクサコントロールシステムは、

上記マルチプレクサシステムにトランスポートストリームパケットの形態として供給される全てのトランスポートストリームパケットに対して、上記トランスポートストリームパケットを識別するためのパケットＩＤを付与することを特徴とする請求の範囲第９８項に記載の限定受信システム。

１００．上記プログラム仕様情報は、

少なくとも、プログラムアソシエーションテーブルと、プログラムマップテーブルと、コンディショナルアクセステーブルとから構成されていることを特徴とする４０請求の範囲第９９項に記載の限定受信システム。

１０１．上記エンコーダ／マルチプレクサコントロールシステムは、

上記プログラムアソシエーションテーブルを含んだトランスポートストリームパケットをＰＡＴパケットとして上記マルチプレクサシステムに供給し、

上記プログラムマップテーブルを含んだトランスポートストリームパケットをＰＭＴパケットとして上記マルチプレクサシステムに供給し、

上記コンディショナルアクセステーブルを含んだトランスポートストリームパケットをＣＡＴパケットとして上記マルチプレクサシステムに供給することを特徴とする請求の範囲第１００項に記載の限定受信システム。

１０２．上記プログラムアソシエーションテーブルは、プログラム番号とそのプログラム番号に対応するＰＭＴパケットのパケットＩＤを指定するためのテーブルであって、

上記プログラムマップテーブルは、プログラムを構成する複数のデータエレメントが含まれるトランスポートストリームパケットのパケットＩＤをそれぞれ指定するためのテーブルであって、上記コンディショナルアクセステーブルは、上記暗号化ＥＭＭパケットのパケットＩＤを指定するためのテーブルであることを特徴とする請求の範囲第１０１項に記載の限定受信システム。

１０３．上記プログラムアソシエーションテーブルには、

プログラムを示すプログラム番号と該プログラムに関連付けられたＰＭＴパケットのパケットＩＤとが記述され、

上記プログラムマップテーブルには、

上記プログラムを示すプログラム番号と、上記プログラムを構成する複数のデ

ータエレメントが含まれるトランスポートストリームパケットが含まれる複数のパケットＩＤと、上記プログラム又は上記データエレメントと関連付けられた暗号化ＥＣＭパケットのパケットＩＤを指定するためのディスクリプタとが記述されている

ことを特徴とする請求の範囲第１０２項に記載の限定受信システム。

１０４．上記プログラムマップテーブル中の上記ディスクリプタが、上記プログラム番号と対応つけられた位置に記述されている場合には、上記ディスクリプタは、上記プログラムを構成する複数のデータエレメントの全てのデータエレメントをスクランブルするためのスクランブルキーを含んだＥＣＭパケットのパケットＩＤを指定し、

上記プログラムマップテーブル中の上記ディスクリプタが、上記プログラムの各データエレメントと対応付けられた位置にそれぞれ記述されている場合には、上記プログラムを構成する複数のデータエレメントの各データエレメントをそれぞれスクランブルするための複数のスクランブルキーを含んだ複数のＥＣＭパケットのパケットＩＤを指定することを特徴とする請求の範囲第１０３項に記載の限定受信システム。

１０５．上記プログラムが、第１のデータエレメントから第ｎのデータエレメントを有し、上記第１のデータエレメントから第ｎのデータエレメントに対して少なくとも１つの異なるスクランブルキーが指定されている場合には、

上記プログラムマップテーブルにおいて、

第１番めのデータエレメントが含まれるトランスポートストリームパケットのパケットＩＤと、上記第１番めのデータエレメントをスクランブルするスクランブルキーを含んだＥＣＭデータを含んだトランスポートストリームパケットのパケットＩＤとが対応付けられて記述され、

第ｎ番めのデータエレメントが含まれるトランスポートストリームパケットの

パケットＩＤと、上記第ｎ番めのデータエレメントをスクランブルするスクランブルキーを含んだＥＣＭデータを含んだトランスポートストリームパケットのパケットＩＤとが対応付けられて記述されていることを特徴とする請求の範囲第１０４項に記載の限定受信システム。

１０６．上記スクランブル手段は、

上記データエレメントを含んだトランスポートストリームパケットのパケットＩＤと上記データエレメントに対して指定されたスクランブルキーとを対応付けた対応テーブルに基いて、上記データエレメントに対して指定されたスクランブルキーを使用して、上記プログラム仕様情報、上記ＥＭＭデータ及び上記ＥＣＭデータはスクランブルせずに、上記データエレメントのみをそれぞれスクランブルすることを特徴とする請求の範囲第１０１項に記載の限定受信システム。

１０７．上記エンコーダ／マルチプレクサコントロールシステムは、

各トランスポートストリームパケットに対して割り当てられたパケットＩＤと、該トランスポートストリームパケットに含まれるデータをスクランブルする際に使用するスクランブルキーとを対応付けたテーブルを生成し、

上記パケットＩＤと上記スクランブルキーとを対応付けたテーブルを、上記マルチプレクサシステムに供給することを特徴とする請求の範囲第１０１項に記載の限定受信システム。

１０８．上記スクランブル手段は、

上記パケットＩＤと上記スクランブルキーとを対応付けたテーブルを参照することによって、上記プログラム仕様情報、上記ＥＭＭデータ及び上記ＥＣＭデータはスクランブルせずに、上記データエレメントのみをスクランブルすることを特徴とする請求の範囲第１０７項に記載の限定受信システム。

１０９．上記スクランブル手段は、

上記多重化手段から上記スクランブル手段に供給されたトランスポートストリームパケットの全てのトランスポートストリームパケットのパケットＩＤを検出し、

上記パケットＩＤと上記スクランブルキーとを対応付けたテーブルに基いて、上記検出されたパケットＩＤに対してスクランブルキーが設定されているか否かを判断し、

上記パケットＩＤに対してスクランブルキーが設定されている場合には、上記パケットＩＤによって示されるトランスポートストリームパケットに含まれるデータエレメントを、設定されたスクランブルキーを使用してスクランブルし、

上記パケットＩＤに対してスクランブルキーが設定されていない場合には、上記パケットＩＤによって示されるトランスポートストリームパケットに含まれるデータはスクランブルしないことを特徴とする請求の範囲第１０７項に記載の限定受信システム。

１１０．上記マルチプレクサシステムは、

上記スクランブルキーを暗号化する第２の暗号化手段と、

上記ＰＡＴパケット、上記ＰＭＴパケット、上記ＣＡＴパケット、上記データエレメントを含んだトランスポートストリームパケット、上記暗号化ＥＭＭパケット及び上記暗号化ＥＣＭパケットをそれぞれバッファリングし、上記多重化手段に対してトランスポートストリームパケットの単位で出力するための複数のバッファ手段とをさらに備えたことを特徴とする請求の範囲第９５項に記載の限定受信システム。

１１１．上記マルチプレクサシステムは、

上記データエレメントを含んだトランスポートストリームパケットをバッファリングするための複数のバッファのバッファ残量を監視し、

上記データエレメントを含んだトランスポートストリームパケットをバッファリングするための複数のバッファのいずれかがオーバーフローしそうなときには、上記ＥＭＭパケットをバッファリングするためのバッファからＥＭＭパケットを上記多重か手段に出力する代わりに、上記オーバフローしそうなバッファから上記データエレメントを含んだトランスポートストリームパケットを上記多重化手段に出力することを特徴とする請求の範囲第１１０項に記載の限定受信システム。

１１２．上記フィルタ手段は、

上記トランスポートストリームに含まれるプログラムアソシエーションテーブルを解析するＰＡＴ解析手段と、

上記トランスポートストリームに含まれるプログラムマップテーブルを解析するＰＭＴ解析手段と、上記トランスポートストリームに含まれるコンディショナルアクセステーブルを解析するＣＡＴ解析手段と、

上記トランスポートストリームに含まれる暗号化ＥＭＭデータを解析するＥＭＭ解析手段と、上記トランスポートストリームに含まれる暗号化ＥＣＭデータを解析するＥＣＭ解析手段とを備えていることを特徴とする請求の範囲第１０９項に記載の限定受信システム。

１１３．上記暗号解読手段は、

上記ＥＭＭデータに含まれる自己の契約情報を記憶するメモリ手段と、

上記トランスポートストリーム中に含まれる暗号化ワークキーと上記顧客管理システムにおいて使用されたマスターキーと同じマスターキーを受取り、上記マスターキーを使用して上記暗号化ワークキーの暗号を解読する第１の暗号解読手段と、

上記トランスポートストリーム中に含まれる暗号化スクランブルキーと上記第１の暗号解読手段から供給された暗号解読されやワークキーとを受取り、上記暗

号解読されたワークキーを使用して上記暗号化スクランブルの暗号を解読する第２の暗号解読手段と、

を備えたことを特徴とする請求の範囲第１０９項に記載の限定受信システム。

１１４．上記デマルチプレクサ手段及び上記フィルタ手段は、

上記トランスポートストリームに含まれるプログラムアソシエーションテーブル及びプログラムマップテーブルを解析することによって、上記プログラムを構成する各データエレメントを含んだトランスポートストリームパケットを識別し、上記データエレメントを含んだトランスポートストリームパケットを適切な上記スクランブラーにそれぞれ出力するように上記デマルチプレクサを制御する請求の範囲第１１３項に記載の限定受信システム。

１１５．上記デマルチプレクサ手段及び上記フィルタ手段は、

上記トランスポートストリームに含まれるコンディショナルアクセステーブルを解析することによって、ＥＭＭデータが含まれるトランスポートストリームパケットを検出し、

上記ＥＭＭデータが含まれるトランスポートストリームから、受信者が契約しているプログラムに関するＥＭＭデータを有するトランスポートストリームパケットのみをフィルタリングし、上記フィルタリングされたトランスポートストリームパケットに含まれるＥＭＭデータを解析することによって、ＥＭＭデータから上記暗号化ワークキーを得ることを特徴とする請求の範囲第１１４項に記載の限定受信システム。

１１６．上記デマルチプレクサ手段及び上記フィルタ手段は、

上記トランスポートストリームに含まれるプログラムアソシエーションテーブル及びこのプログラムアソシエーションテーブルによって指定されたプログラムマップテーブルを解析することによって、上記プログラムを構成する複数のデー

タエレメント及び上記ＥＣＭデータを含んだトランスポートストリームパケットをそれぞれ検出し、

上記複数のデータエレメントを含んだトランスポートストリームパケットをそれぞれ上記デスクランブラーに供給すると共に、上記ＥＣＭデータを含んだトランスポートストリームパケットを受け取るように、上記デマルチプレクサを制御することを特徴とする請求の範囲第１１３項に記載の限定受信システム。

１１７．上記デマルチプレクサ手段及び上記フィルタ手段は、

上記デマルチプレクサから供給された暗号化ＥＣＭデータを含んだトランスポートストリームパケットから、受信者が契約しているプログラム又はデータエレメントに関する暗号化ＥＣＭデータを有するトランスポートストリームパケットのみをフィルタリングし、

上記フィルタリングされたトランスポートストリームパケットに含まれる暗号化ＥＣＭデータを解析することによって、上記暗号化ＥＣＭデータから上記暗号化スクランブルキーを得ることを特徴とする請求の範囲第１１６項に記載の限定受信システム。

１１８．上記プログラムマップテーブルのシンタックスにおいて、上記プログラム番号と上記暗号化ＥＣＭパケットのパケットＩＤとが対応付けられて記述されている場合には、

上記フィルタ手段は、上記パケットＩＤによって指定された暗号化ＥＣＭパケットに含まれている暗号化スクランブルキーを、上記プログラムに対応する暗号化スクランブルキーとして上記暗号解読手段に供給し、上記プログラムマップテーブルのシンタックスにおいて、上記プログラムを構成する複数のデータエレメントと上記複数の暗号化ＥＣＭパケットのパケットＩＤとがそれぞれ対応付けられて記述されている場合には、

上記フィルタ手段は、上記複数のパケットＩＤによって指定された暗号化ＥＣ

Mパケットに含まれるそれぞれ異なる複数のスクランブルキーを、上記複数のデータエレメントに対応する暗号化スクランブルキーとして上記暗号解読手段に供給する

ことを特徴とする請求の範囲第１１７項に記載の限定受信システム。

１１９．上記暗号解読手段は、

上記フィルタ手段から上記プログラムに対応する暗号化スクランブルキーが供給された場合には、供給された暗号化スクランブルキーの暗号を解読し、上記プログラムを構成する複数のデータエレメントに対応する複数のデスクランブラーに対して同じスクランブルキーをそれぞれ供給し、

上記フィルタ手段から上記複数のデータエレメントにそれぞれ対応する複数の暗号化スクランブルキーが供給された場合には、供給された複数の暗号化スクランブルキーの暗号をそれぞれ解読し、上記複数のデータエレメントのうち契約しているデータエレメントに対応する複数のデスクランブラーに対して、それぞれ異なるスクランブルキーを供給する請求の範囲第１１８項に記載の限定受信システム。

１２０．トランスポートストリームパケット構成の複数のデータエレメントからなるプログラムデータの上記各トランスポートストリームパケットを多重化してなる多重化データを受信するデータ受信装置において、

上記データエレメントごとに対応するスクランブルキーを上記多重化データから抽出するスクランブルキー抽出手段と、

上記スクランブルキー抽出手段によつて抽出されたスクランブルキーを用いて上記多重化データに含まれる上記各データエレメントごとのトランスポートストリームパケットをデスクランブルするデスクランブル手段と

を具えることを特徴とするデータ受信装置。

１２１．上記データ受信装置は、

上記スクランブルキー抽出手段によって抽出された暗号化済の上記スクランブルキーを上記多重化データと共に受信されたワークキーを用いて解読する第１の暗号解読手段を具え、上記第１の暗号解読手段によつて解読された上記スクランブルキーを用いて上記トランスポートストリームパケットをデスクランブルする

ことを特徴とする請求の範囲第１２０項に記載のデータ受信装置。

１２２．上記データ受信装置は、

上記多重化データと共に受信された暗号化済の上記ワークキーを予め記憶されているマスターキーを用いて解読する第２の暗号解読手段を具え、上記第２の暗号解読手段によつて解読された上記ワークキーを用いて上記スクランブルキーを解読する

ことを特徴とする請求の範囲第１２０項に記載のデータ受信装置。

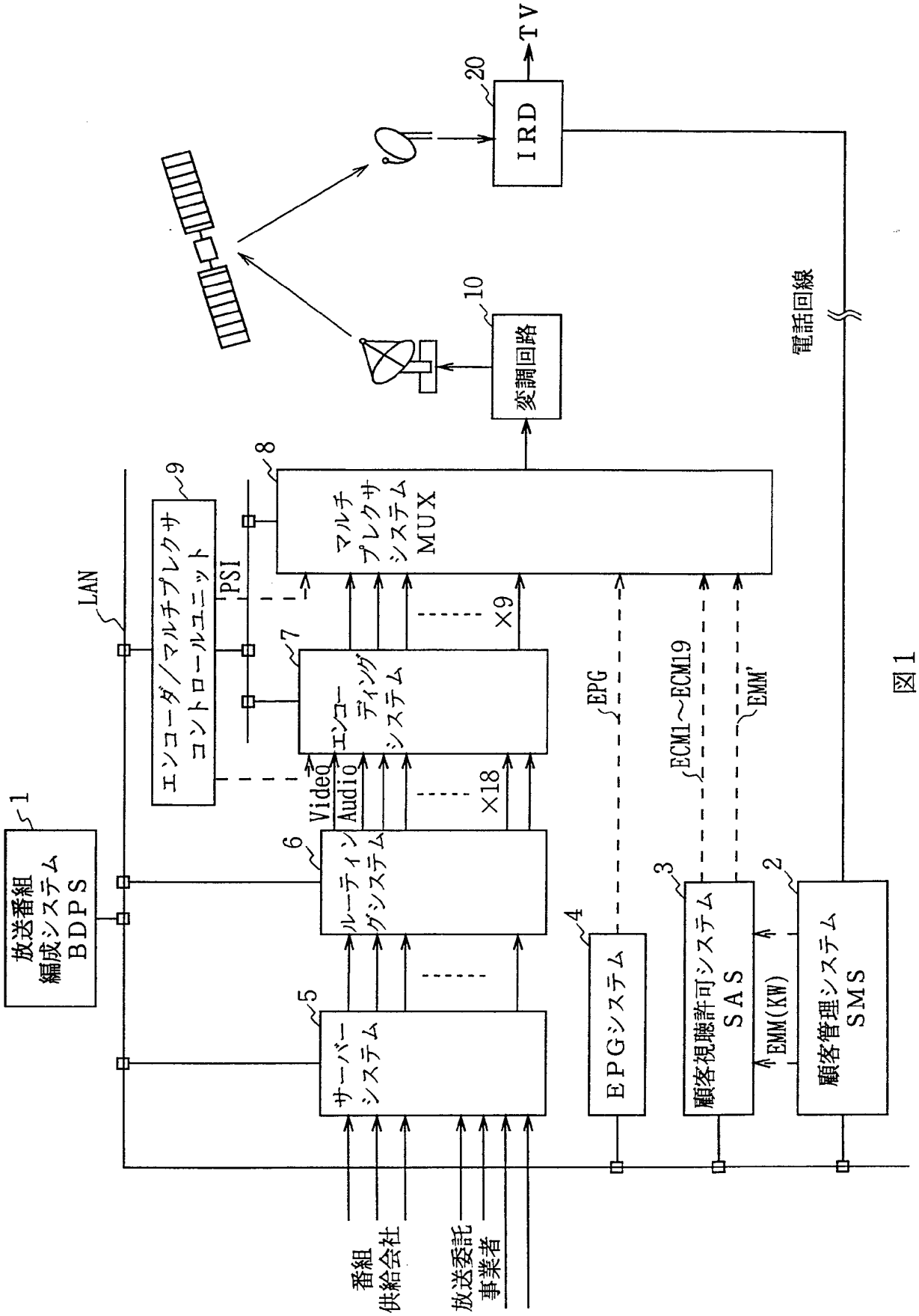
TV
20
IRD
10
変調回路
電話回線
8
マルチプレクサシステム MUX
9
エンコーダ／マルチプレクサコントロールユニット
LAN
PSI
7
エンコーディングシステム
×9
Video
Audio
×18
6
ルーティングシステム
1
放送番組編成システム BDPS
5
サーバーシステム
4
EPGシステム
EPG
3
顧客視聴許可システム SAS
ECM1～ECM19
EMM'
EMM(KW)
2
顧客管理システム SMS
番組供給会社
放送委託事業者

図1

Program number	Video	Main Audio	Sub Audio	Private
1	Ks1		---	---
2	Ks2		Ks3	Ks4
3	Ks5	Ks6	---	---
4	Ks7	Ks8	Ks9	Ks10
5	Ks11			
6	Ks12		---	---
7	Ks13			Ks14
8	Ks15			
9	Ks16	Ks17	Ks18	Ks19

図2

ＰＩＤ値	パケット内に記録される情報
０ｘ０００Ｏ	ＰＡＴ
０ｘ０００１	ＣＡＴ
０ｘ０００２～０ｘ０００Ｆ	Ｒｅｓｅｒｖｅｄ
０ｘ００１０	ＮＩＴ、ＳＴ
０ｘ００１１	ＳＤＴ、ＢＡＴ、ＳＴ
０ｘ００１２	ＥＩＴ、ＳＴ
０ｘ００１３	ＲＳＴ、ＳＴ
０ｘ００１４	ＴＤＴ
０ｘ００１５～０ｘ００１Ｆ	Ｒｅｓｅｒｖｅｄ
０ｘ００２０～０ｘ１ＦＦＥ	ＰＭＴ、ビデオ／オーディオ等のストリーム
０ｘ１ＦＦＦ	Ｎｕｌｌ　Ｐａｃｋｅｔ

図３

ＰＩＤテーブル

パケット種類	ＰＩＤ値	スクランブルキー
ＰＡＴパケット	０×０００００ （固定値）	― ― ―
・ ・ ・	・ ・ ・	
ＰＭＴ１パケット	０×０１００	― ― ―
ＰＭＴ２パケット	０×０１０１	― ― ―
・ ・ ・ ・	・ ・ ・ ・	
ＥＣＭ１パケット	０×０３００	― ― ―
・ ・	・ ・	
ＥＣＭ２パケット	０×０３５１	― ― ―
ＥＣＭ２パケット	０×０３５２	― ― ―
ＥＣＭ３パケット	０×０３５３	― ― ―
ＥＣＭ４パケット	０×０３５４	― ― ―
・ ・ ・ ・	・ ・ ・ ・	
Video[1]パケット	０×０５００	Ｋｓ１
Main_Audio[1]パケット	０×０５０１	Ｋｓ１
Video[2]パケット	０×０５０２	Ｋｓ２
Main_Audio[2]パケット	０×０５０３	Ｋｓ２
Sub_Audio[2]パケット	０×０５０４	Ｋｓ３
Private[2]パケット	０×０５０５	Ｋｓ４
・ ・ ・ ・	・ ・ ・ ・	
ＣＡＴパケット	０×０００１ （固定値）	― ― ―
・ ・ ・ ・	・ ・ ・ ・	
ＥＭＭパケット	０×０７００	― ― ―
・ ・ ・	・ ・ ・	

図４

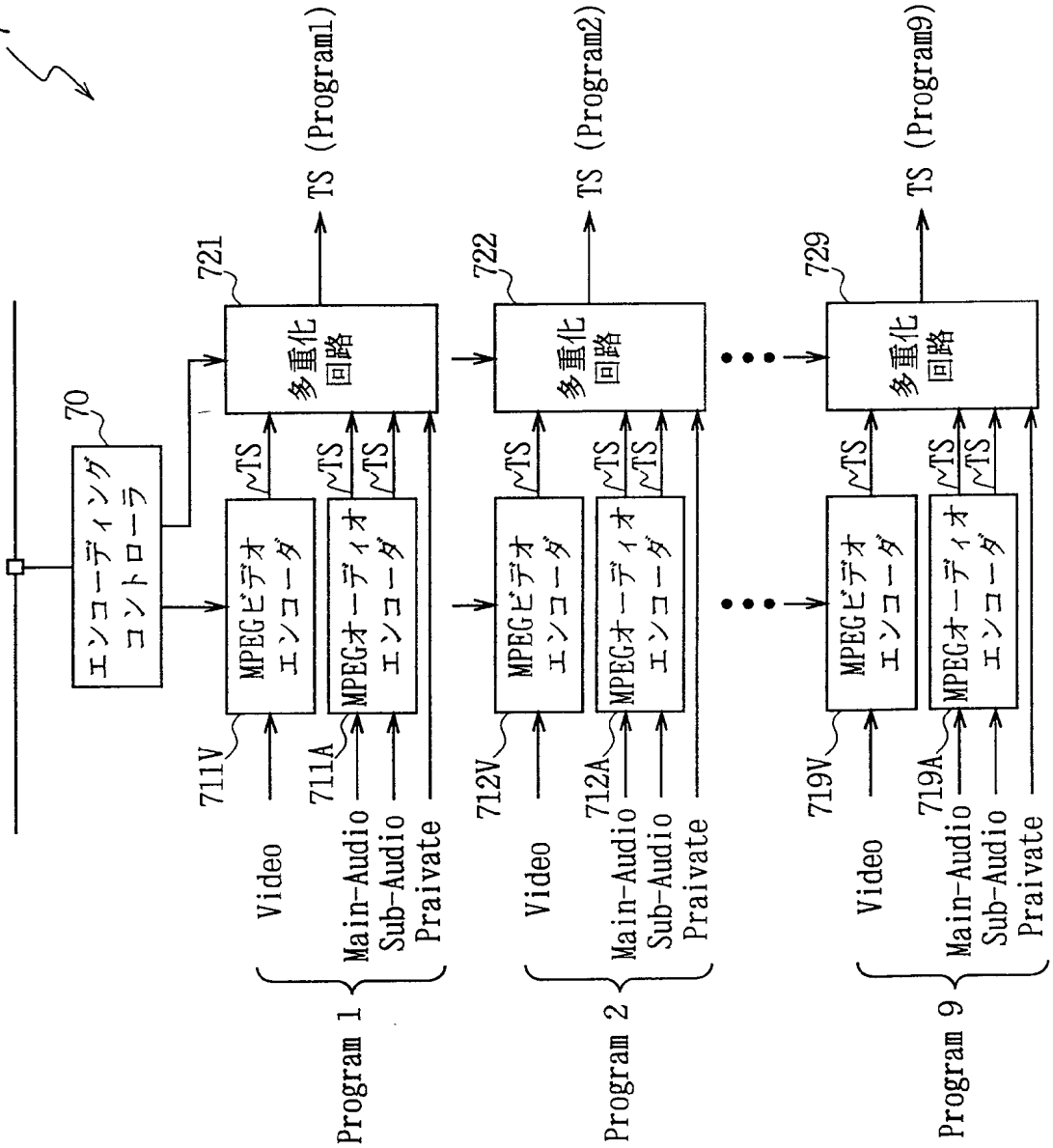
7
70
エンコーディング
コントローラ
721
722
729
多重化
回路
TS (Program1)
TS (Program2)
TS (Program9)
MPEGビデオ
エンコーダ
MPEGオーディオ
エンコーダ
TS
711V
711A
712V
712A
719V
719A
Video
Main-Audio
Sub-Audio
Praivate
Program 1
Program 2
Program 9

図5

シンタックス	ビット数	ニーモニック
transport packet(){		
sync_byte	8	bslbf
transport_error_indicator	1	bslbf
payload_unit_start_indicator	1	bslbf
transport_priority	1	bslbf
PID	13	uimsbf
transport_scrambling_control	2	bslbf
adaptation_field_control	2	bslbf
continuity_counter	4	uimsbf
if(adaptation_field_control==' || adaptation_field_control=='11'{		
adaptation filed()		
}		
if(adaptation_field_control==' || adaptation_field_control=='11'{		
for(i=0;i<N;i++){		
data_byte	8	bslbf
}		
}		
}		

図6

シンタックス	ビット数	ニーモニック
adaptation_field(){		
adaptation_filed_length	8	uimsbf
if(adaptation_field_length>0){		
discontinuity_indicator	1	bslbf
random access_indicator	1	bslbf
elementary_stream_priority_indicator	1	bslbf
PCR_flag	1	bslbf
OPCR_flag	1	bslbf
splicing_point_flag	1	bslbf
transport_private_data_flag	1	bslbf
adaptation_field_extension_flag	1	bslbf
if(PCR_flag=='1'){		
program_clock_reference_base	33	uimsbf
reserved	6	bslbf
program_clock_reference_extension	9	uimsbf
}		
if(OPCR_flag=='1'){		
original_program_clock_reference_base	33	uimsbf
reserved	6	bslbf
original_program_clock_reference_extension	9	uimsbf
}		
if(splicing_point_flag=='1'){		
splice_countdown	8	tcimsbf
}		
if(transport_private_data_flag=='1'){		
transport_private_data_length	8	uimsbf
for(i=0;i<transport_private_data_length;i++;){		
private_data_byte	8	bslbf
}		
}		
if(adaptation_field_extension_flag=='1'){		
adaptation_field_extension_length	8	uimsbf
ltw_flag	1	bslbf
piecewise_rate_flag	1	bslbf
seamless_splice_flag	1	bslbf

図7

```
            reserved                                    5       bslbf
            if(ltw_flag=='1'){
                ltw_valid_flag                          1       bslbf
                ltw_offset                             15       uimsbf
            }
            if(piecewise_rate_flag=='1'){
                reserved                                2       bslbf
                piecewise_rate                         22       uimsbf
            }
            if(seamless_splice_flag=='1'){
                splice_type                             4       bslbf
                DTS_next_AU[32..30]                     3       bslbf
                market_bit                              1       bslbf
                DTS_next_AU[29..15]                    15       bslbf
                marker_bit                              1       bslbf
                DTS_next_AU[14..0]                     15       bslbf
                marker_bit                              1       bslbf
            }
            for(i=0;i<N;i++){
                reserved                                8       bslbf
            }
    }
    for(i=0;i<N;i++){
            stuffing_byte                               8       bslbf
    }
  }
}
```

図8

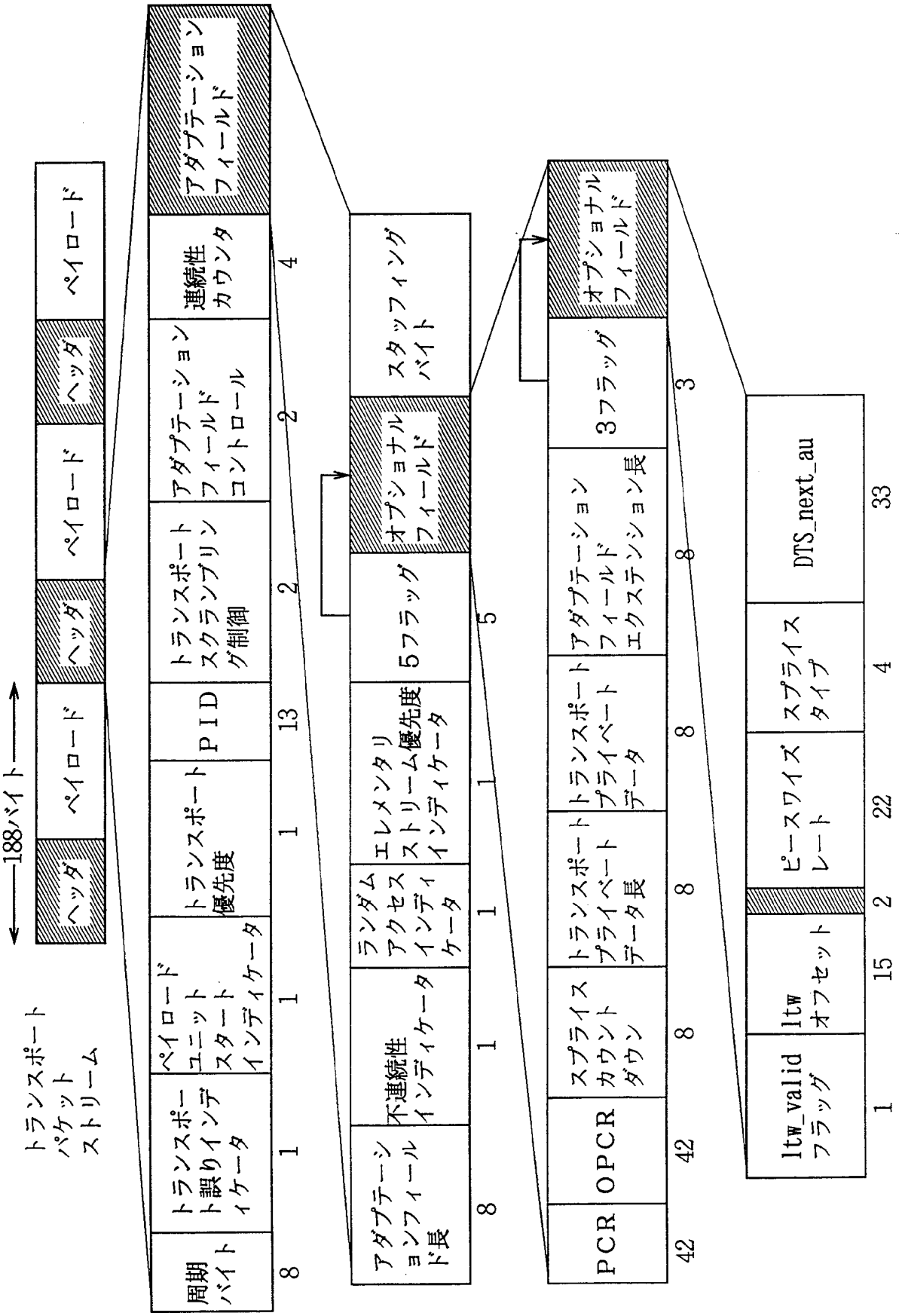
トランスポート
パケット
ストリーム
188バイト
ヘッダ
ペイロード
ヘッダ
ペイロード
ヘッダ
ペイロード
周期
バイト
トランスポート誤りインディケータ
ペイロードユニットスタートインディケータ
トランスポート優先度
PID
トランスポートスクランブリング制御
アダプテーションフィールドコントロール
連続性カウンタ
アダプテーションフィールド
8
1
1
1
13
2
2
4
アダプテーションフィールド長
不連続性インディケータ
ランダムアクセスインディケータ
エレメンタリストリーム優先度インディケータ
5フラッグ
オプショナルフィールド
スタッフィングバイト
8
1
1
1
5
PCR
OPCR
スプライスカウントダウン
トランスポートプライベートデータ長
トランスポートプライベートデータ
アダプテーションフィールドエクステンション長
3フラッグ
オプショナルフィールド
42
42
8
8
8
3
ltw_valid
フラッグ
ltw
オフセット
ピースワイズレート
スプライスタイプ
DTS_next_au
1
15
2
22
4
33

図9

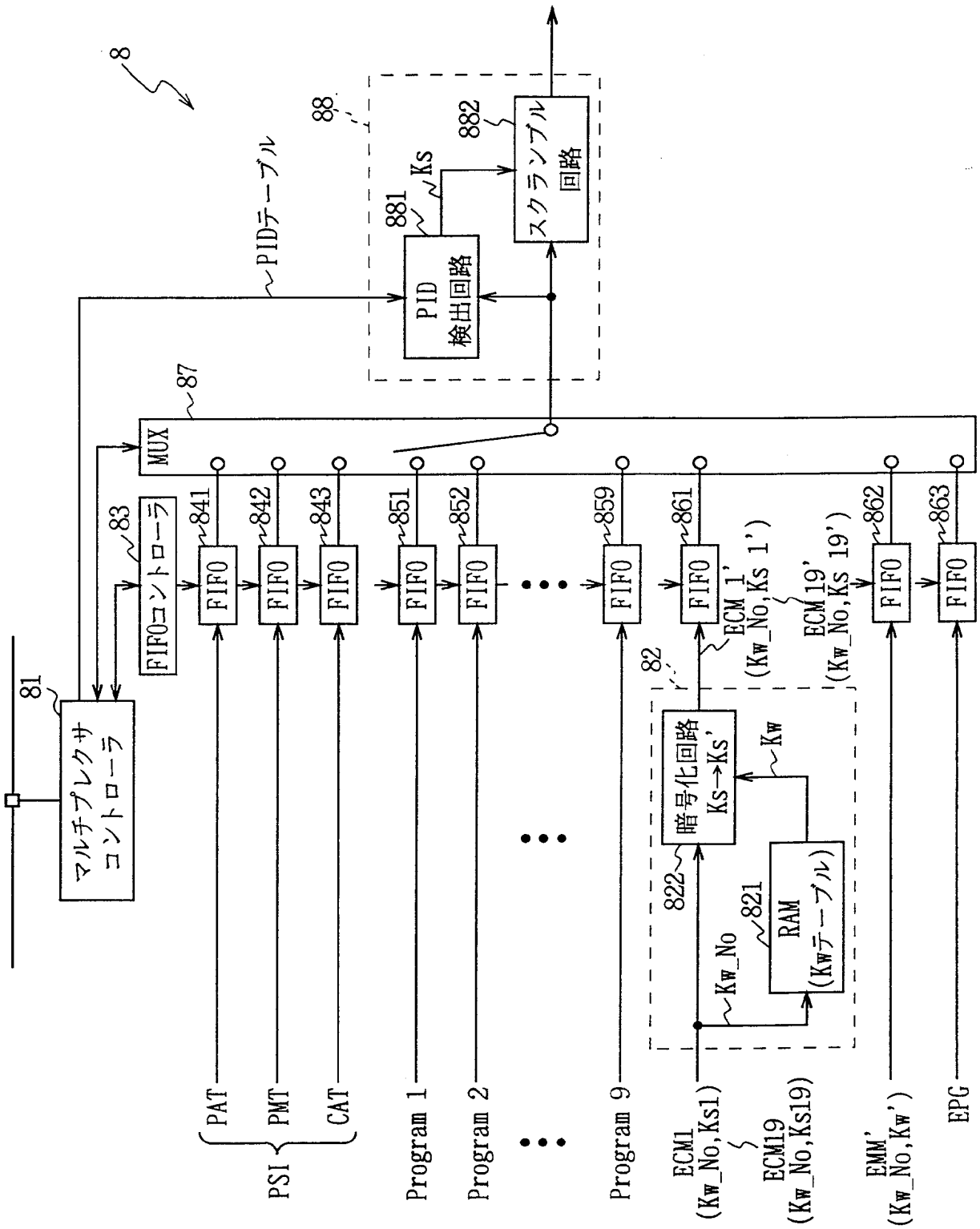
8
88
PIDテーブル
881
Ks
882
スクランブル回路
PID検出回路
87
MUX
83
FIFOコントローラ
841
842
843
851
852
859
861
862
863
FIFO
81
マルチプレクサコントローラ
82
暗号化回路 Ks→Ks'
Kw
822
821
RAM (Kwテーブル)
Kw_No
ECM_1' (Kw_No,Ks 1')
ECM_19' (Kw_No,Ks 19')
PAT
PMT
CAT
PSI
Program 1
Program 2
Program 9
ECM1 (Kw_No,Ks1)
ECM19 (Kw_No,Ks19)
EMM' (Kw_No,Kw')
EPG

図１０

構造名	割り当てPID #	説明
プログラム アソシエーション テーブル(PAT)	0x00	プログラム番号とプログラムマップ テーブルPIDを割り当てる
プログラムマップ テーブル(PMT)	PATで割り当て	一つ以上のプログラムの構成要素の PIDを規定する
網情報テーブル (NIT)	PATで割り当て	FDM周波数や中継器番号などの 物理的なネットワークパラメータ
条件付きアクセス テーブル(CAT)	0x01	一つ以上の（プライベートの） EMMストリームにそれぞれ 固有のPID値を割り当てる

図１１

シンタックス	ビット数	ニーモニック
program_association section() {		
table_id	8	uimsbf
section_syntax_indicator	1	bslbf
'0'	1	bslbf
reserved	2	bslbf
section_length	12	uimsbf
transport_stream_id	16	uimsbf
reserved	2	bslbf
version_number	5	uimsbf
current_next_indicator	1	bslbf
section_number	8	uimsbf
last_section_number	8	uimsbf
for(i=0; i<N;i++) {		
program_number	16	uimsbf
reserved	3	bslbf
if(program number == '0')		
{		
network_PID	13	uimsbf
}		
else {		
program_map_PID	13	uimsbf
}		
}		
CRC32	32	rpchof
}		

図１２

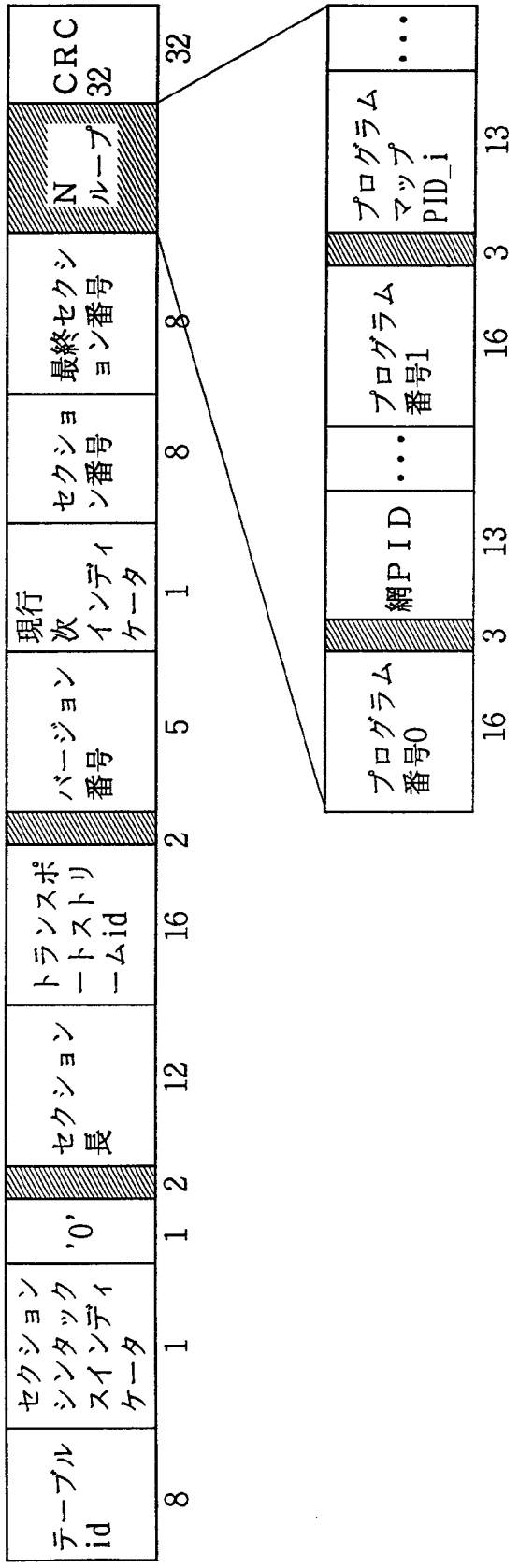
テーブル id
8
セクションシンタックスインディケータ
1
'0'
1
セクション長
2
12
トランスポートストリームid
16
バージョン番号
2
5
現行次インディケータ
1
セクション番号
8
最終セクション番号
8
N ループ
CRC 32
32
プログラム番号0
16
網PID
3
13
・・・
プログラム番号1
16
プログラムマップ PID_i
3
13
・・・

図13

値	説　　明
0x00	プログラムアソシエーションセクション
0x01	条件付きアクセスセクション(CA section)
0x02	プログラムマップセクション
0x03-0x3F	ITU-T 勧告 H.222.0	ISO/IEC 13818 予約された
0x40-0xFE	ユーザープライベート
0xFF	禁止

図１４

シンタックス	ビット数	ニーモニック
TS_program_map_section() {		
table_id	8	uimsbf
section_syntax_indicator	1	bslbf
'0'	1	bslbf
reserved	2	bslbf
section_length	12	uimsbf
program_number	16	uimsbf
reserved	2	bslbf
version_number	5	uimsbf
current_next_indicator	1	bslbf
section_number	8	uimsbf
last_section_number	8	uimsbf
reserved	3	bslbf
PCR_PID	13	uimsbf
reserved	4	bslbf
program_info_length	12	uimsbf
for(i=0; i<N;i++) {		
descriptor()		
}		
for(i=0; i<N;i++) {		
stream_type	8	uimsbf
reserved	3	bslbf
elementary_PID	13	uimsbf
reserved	4	bslbf
ES_info_length	12	uimsbf
for(i=0; i<N2; i++) {		
descriptor()		
}		
}		
CRC32	32	rpchof
}		

図１５

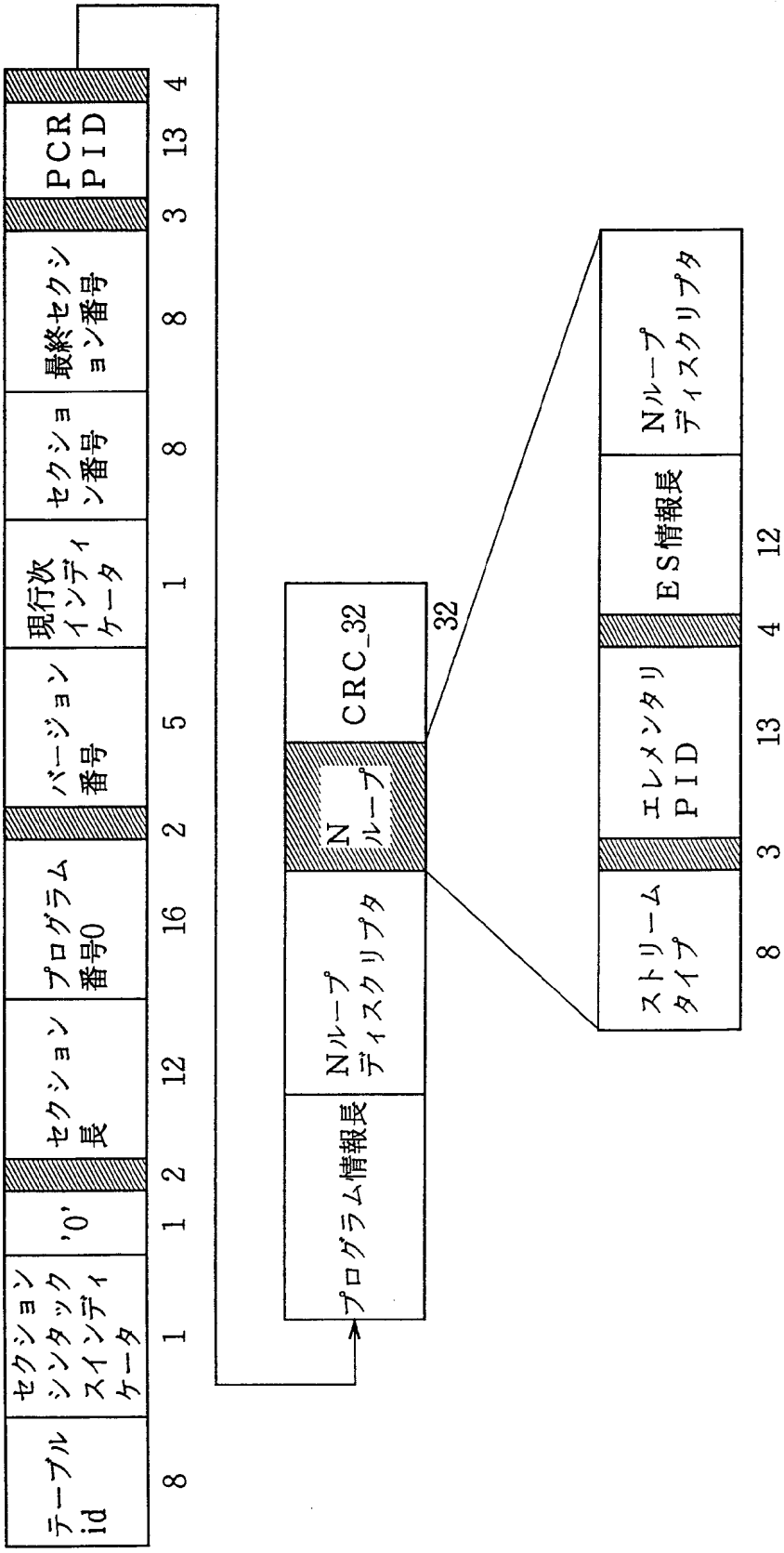
テーブル id
8
セクション シンタックス インディケータ
1
'0'
1
セクション長
2
12
プログラム番号0
16
バージョン番号
2
5
現行次インディケータ
1
セクション番号
8
最終セクション番号
8
PCR PID
3
13
4
プログラム情報長
Nループ ディスクリプタ
Nループ
CRC_32
32
ストリームタイプ
8
エレメンタリ PID
3
13
ES情報長
4
12
Nループ ディスクリプタ

図16

シンタックス	ビット数	ニーモニック
CA_section() {		
table_id	8	uimsbf
section_syntax_indicator	1	bslbf
'0'	1	bslbf
reserved	2	bslbf
section_length	12	uimsbf
reserved	18	bslbf
version_number	5	uimsbf
current_next_indicator	1	bslbf
section_number	8	uimsbf
last_section_number	8	uimsbf
for(i=0; i<N;i++) {		
descriptor()		
}		
CRC32	32	rpchof
}		

図１７

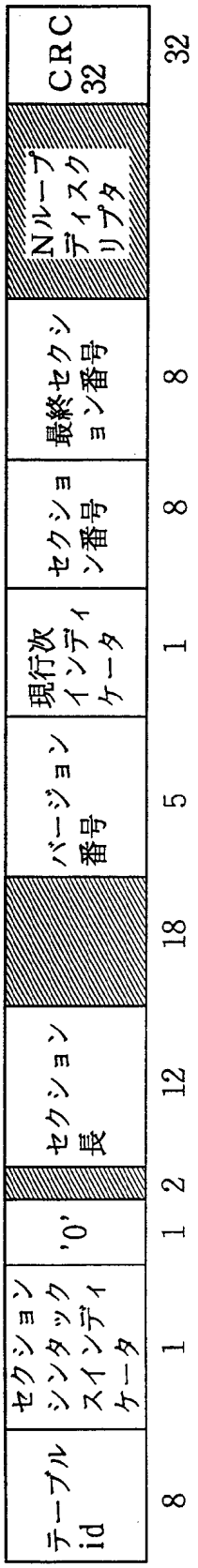
テーブル id
8
セクション シンタックス インディケータ
1
'0'
1
2
セクション長
12
18
バージョン番号
5
現行次インディケータ
1
セクション番号
8
最終セクション番号
8
Nループ ディスク リプタ
CRC 32
32

図18

シンタックス	ビット数	ニーモニック
CA_descriptor() {		
descriptor_tag	8	uimbf
descriptor_length	8	uimsbf
CA_system_ID	16	uimsbf
reserved	3	bslbf
CA_PID	13	uimsbf
for(i=0; i<N;i++) {		
private_data_byte	8	uimsbf
}		
}		

図１９

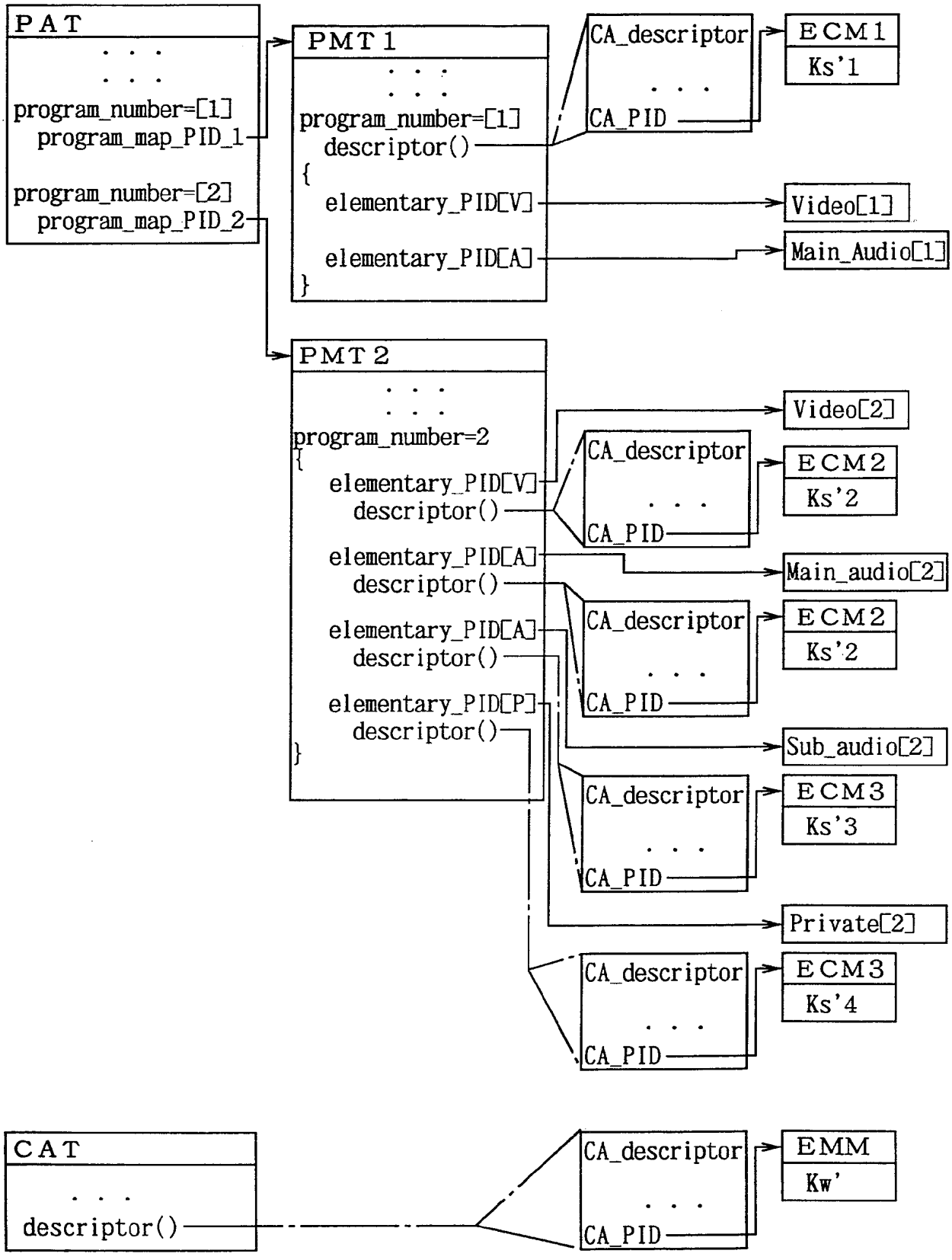
PAT
program_number=[1]
program_map_PID_1
program_number=[2]
program_map_PID_2
PMT 1
program_number=[1]
descriptor()
{
elementary_PID[V]
elementary_PID[A]
}
CA_descriptor
CA_PID
ECM1
Ks'1
Video[1]
Main_Audio[1]
PMT 2
program_number=2
{
elementary_PID[V]
descriptor()
elementary_PID[A]
descriptor()
elementary_PID[A]
descriptor()
elementary_PID[P]
descriptor()
}
Video[2]
ECM2
Ks'2
Main_audio[2]
Sub_audio[2]
ECM3
Ks'3
Private[2]
ECM3
Ks'4
CAT
descriptor()
EMM
Kw'

図２０

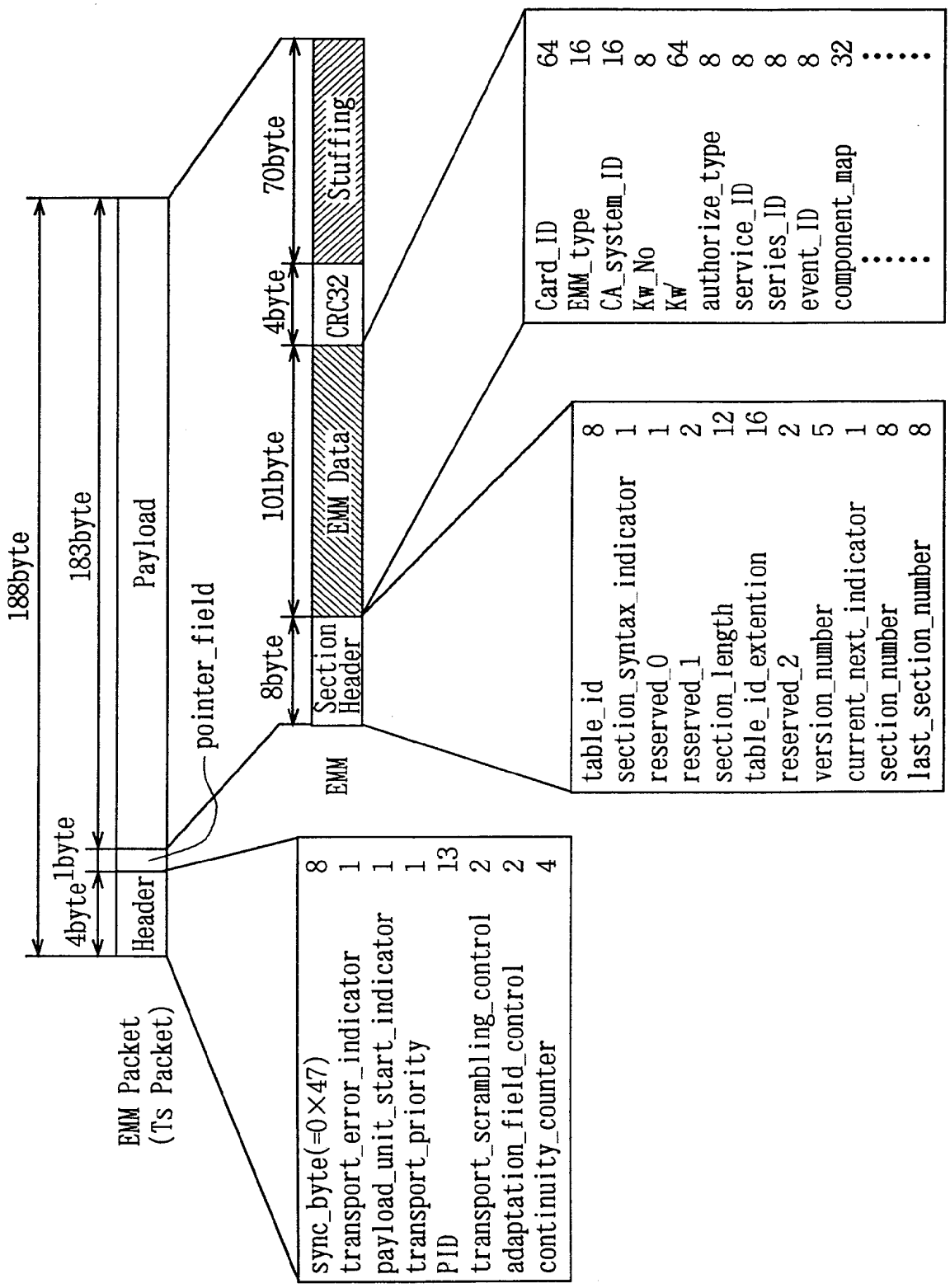
188byte
183byte
4byte
1byte
Header
Payload
pointer_field
EMM Packet
(Ts Packet)
8byte
101byte
4byte
70byte
Section Header
EMM Data
CRC32
Stuffing
EMM
sync_byte(=0×47) 8
transport_error_indicator 1
payload_unit_start_indicator 1
transport_priority 1
PID 13
transport_scrambling_control 2
adaptation_field_control 2
continuity_counter 4
table_id 8
section_syntax_indicator 1
reserved_0 1
reserved_1 2
section_length 12
table_id_extention 16
reserved_2 2
version_number 5
current_next_indicator 1
section_number 8
last_section_number 8
Card_ID 64
EMM_type 16
CA_system_ID 16
Kw_No 8
Kw' 64
authorize_type 8
service_ID 8
series_ID 8
event_ID 8
component_map 32
.....
.....

図21

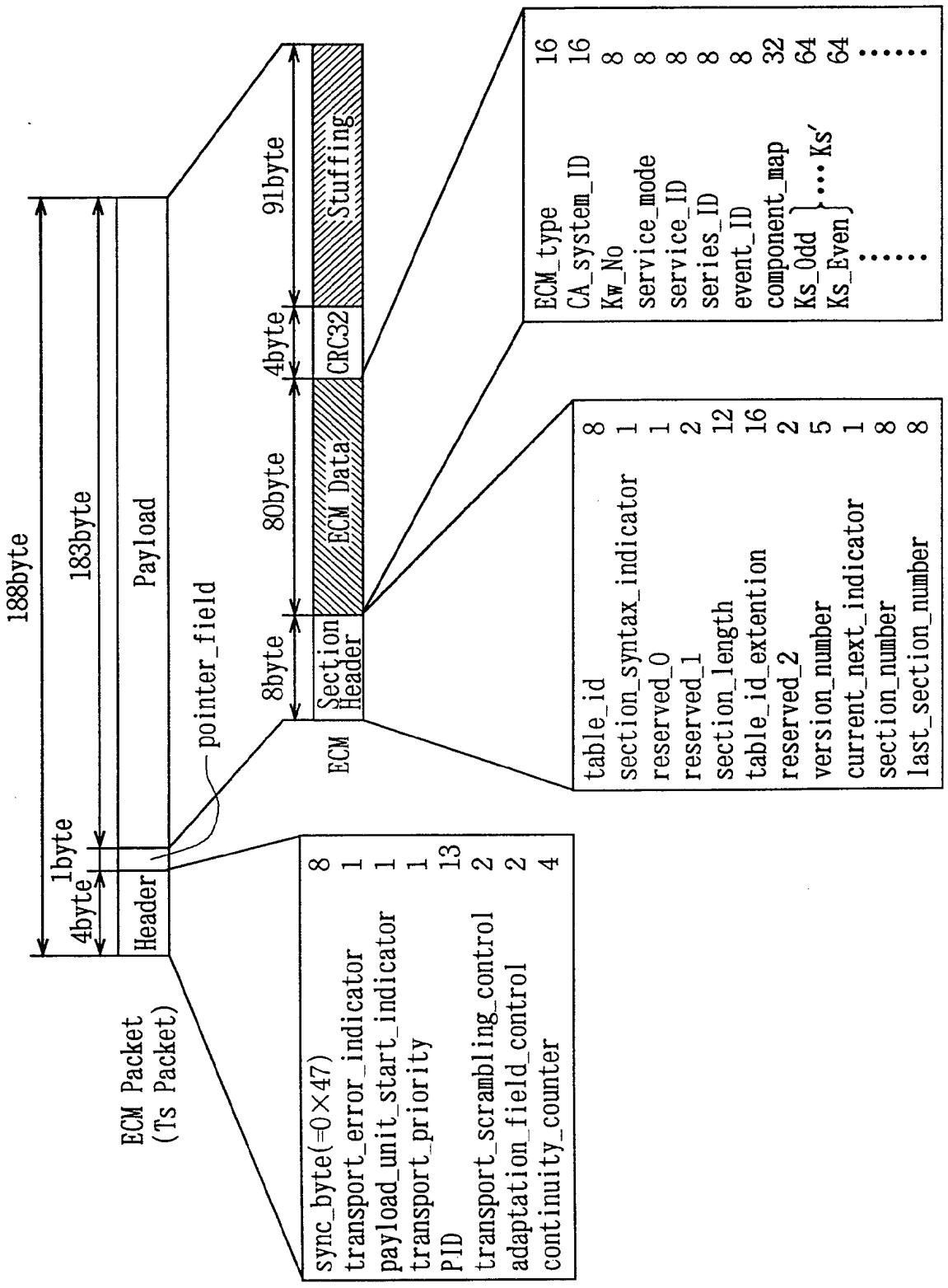
188byte
183byte
1byte
4byte
Header
Payload
pointer_field
ECM Packet
(Ts Packet)
8byte
80byte
4byte
91byte
Section Header
ECM Data
CRC32
Stuffing
ECM
sync_byte(=0×47) 8
transport_error_indicator 1
payload_unit_start_indicator 1
transport_priority 1
PID 13
transport_scrambling_control 2
adaptation_field_control 2
continuity_counter 4
table_id 8
section_syntax_indicator 1
reserved_0 1
reserved_1 2
section_length 12
table_id_extention 16
reserved_2 2
version_number 5
current_next_indicator 1
section_number 8
last_section_number 8
ECM_type 16
CA_system_ID 16
Kw_No 8
service_mode 8
service_ID 8
series_ID 8
event_ID 8
component_map 32
Ks_Odd } ··· Ks'
Ks_Even } 64
64

図22

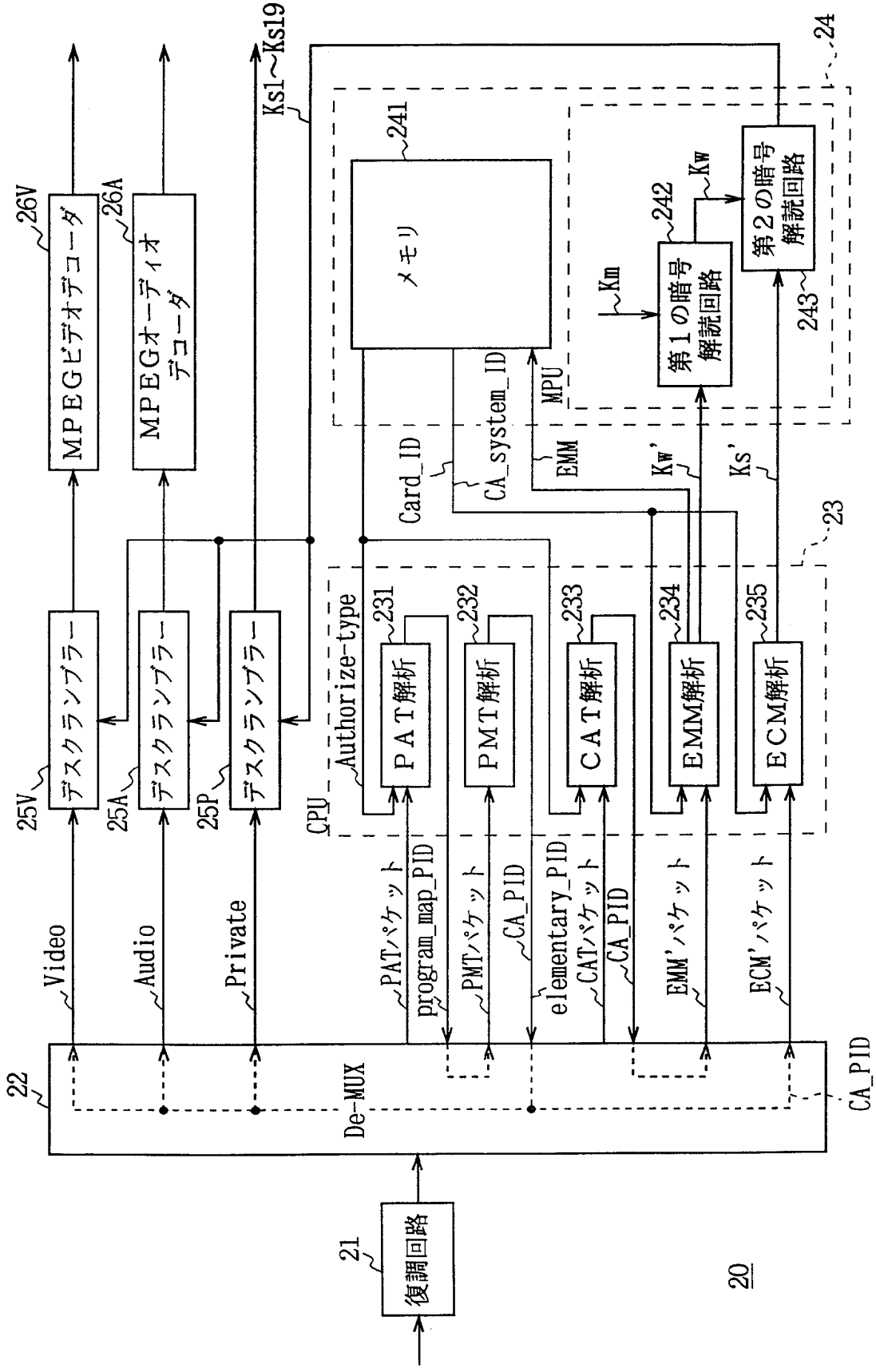
20
21
復調回路
22
De-MUX
CA_PID
23
24
25V
25A
25P
26V
26A
デスクランブラー
デスクランブラー
デスクランブラー
MPEGビデオデコーダ
MPEGオーディオデコーダ
Video
Audio
Private
Ks1～Ks19
CPU
Authorize-type
241
メモリ
Card_ID
CA_system_ID
MPU
EMM
Km
242
第１の暗号解読回路
Kw
第２の暗号解読回路
243
Kw'
Ks'
231
PAT解析
232
PMT解析
233
CAT解析
234
EMM解析
235
ECM解析
PATパケット
program_map_PID
PMTパケット
CA_PID
elementary_PID
CATパケット
CA_PID
EMM'パケット
ECM'パケット

図２３

符　号　の　説　明

１……放送番組編成システム、２……顧客管理システム、３……顧客視聴許可システム、４……ＥＰＧシステム、５……サーバーシステム、６……ルーティングシステム、７……エンコーディングシステム、８……マルチプレクサシステム、９……エンコーダ／エルチプレクサコントロールユニット、１０……変調回路、２０……ＩＲＤ、２１……復調回路、２２……デマルチプレクサ、２４……ＩＣカード、２５Ｖ、２５Ａ、２５Ｐ……デフクランブラー、２６Ｖ……ＭＰＥＧビデオデコーダ、２６Ａ……ＭＰＥＧオーディオデコーダ、７０……エンコーディングコントローラ、２４１……メモリ、２４２……第１の暗号解読回路、２４３……第２の暗号解読回路、７１１Ｖ～７１９Ｖ……ＭＰＥＧビデオエンコーダ、７１１Ａ～７１９Ａ……ＭＰＥＧオーディオエンコーダ、７２１～７２９……多重化回路、８４１～８６３……バッファメモリ（ＦＩＦＯ）。

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP98/03127

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[6] H04N7/16, 7/167, 08, H04K1/04, H04L12/18

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[6] H04N7/16, 7/167, 08, H04K1/04, H04L12/18

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1937-1996 Jitsuyo Shinan Toroku Koho 1996-1998
Kokai Jitsuyo Shinan Koho 1971-1998

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 9-511369, A (Scientific Atlanta, Inc.), 11 November, 1997 (11. 11. 97) & WO, 95/26597, A1 & AU, 9472209, A & AU, 687844, B & US, 5420866, A	1-7, 12-26, 28-56, 58-89, 91-110, 112-122
A		8-11, 27, 57, 90, 111
Y	JP, 8-340541, A (Sony Corp.), 24 December, 1996 (24. 12. 96) (Family: none)	1-7, 12-26, 28-56, 58-89, 91-110, 112-122
A		8-11, 27, 57, 90, 111
Y	JP, 9-51520, A (Sony Corp.), 18 February, 1997 (18. 02. 97) (Family: none)	1-7, 12-26, 28-56, 58-89, 91-110, 112-122

[x] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
7 October, 1998 (07. 10. 98)	20 October, 1998 (20. 10. 98)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP98/03127

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A		8-11, 27, 57, 90, 111
Y	JP, 9-284763, A (Sony Corp.),	8, 9
A	31 October, 1997 (31. 10. 97) (Family: none)	1-7, 10-122
Y	JP, 9-312625, A (Sony Corp.),	8, 9
A	2 December, 1997 (02. 12. 97) (Family: none)	1-7, 10-122
Y	JP, 10-126371, A (Sony Corp.),	8, 9
A	15 May, 1998 (15. 05. 98) (Family: none)	1-7, 10-122
A	JP, 7-202884, A (Sony Corp.), 4 August, 1995 (04. 08. 95) (Family: none)	1-122
A	JP, 8-289277, A (Sony Corp.), 1 November, 1996 (01. 11. 96) (Family: none)	1-122
A	JP, 8-340514, A (Sony Corp.), 24 December, 1996 (24. 12. 96) (Family: none)	1-122
A	JP, 9-9241, A (Sony Corp.), 10 January, 1997 (10. 01. 97) (Family: none)	1-122
A	JP, 9-46672, A (Sony Corp.), 14 February, 1997 (14. 02. 97) (Family: none)	1-122
A	JP, 9-46681, A (Sony Corp.), 14 February, 1997 (14. 02. 97) (Family: none)	1-122
A	JP, 9-284762, A (Sony Corp.), 31 October, 1997 (31. 10. 97) (Family: none)	1-122
A	JP, 9-307542, A (Sony Corp.), 28 November, 1997 (28. 11. 97) (Family: none)	1-122
A	JP, 9-322161, A (K.K. Ekushingu), 12 December, 1997 (12. 12. 97) (Family: none)	1-122

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP98/03127

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The group of inventions disclosed in claims 1-7 and 12-122 relates to encryption of data elements, whereas the group of inventions disclosed in claims 8-11 relates to time division multiplexing of data elements, and these two groups of inventions are not considered as relating to a group of inventions so linked as to form a single general inventive concept.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ９８／０３１２７

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ ｃｌ[6] Ｈ０４Ｎ７／１６，７／１６７，０８，Ｈ０４Ｋ１／０４，Ｈ０４Ｌ１２／１８

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ ｃｌ[6] Ｈ０４Ｎ７／１６，７／１６７，０８，Ｈ０４Ｋ１／０４，Ｈ０４Ｌ１２／１８

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９３７－１９９６年
日本国公開実用新案公報	１９７１－１９９８年
日本国実用新案登録公報	１９９６－１９９８年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ，９－５１１３６９，Ａ（サイエンテイフイクーアトランタ・インコーポレーテツド），１１．１１月．１９９７（１１．１１．９７） ＆　ＷＯ，９５／２６５９７，Ａ１ ＆　ＡＵ，９４７２２０９，Ａ ＆　ＡＵ，６８７８４４，Ｂ	1-7, 12-26, 28-56, 58-89, 91-110, 112-122
Ａ	＆　ＵＳ，５４２０８６６，Ａ	8-11, 27, 57, 90, 111

☒ Ｃ欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」先行文献ではあるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 ０７．１０．９８	国際調査報告の発送日 20.10.98
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 山崎　達也　　５Ｃ　８１２１ 電話番号　０３－３５８１－１１０１　内線　３５４１

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９２年７月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ９８／０３１２７

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ，８－３４０５４１，Ａ（ソニー株式会社），２４．１２月．１９９６（２４．１２．９６）（ファミリーなし）	1-7, 12-26, 28-56, 58-89, 91-110, 112-122
Ａ		8-11, 27, 57, 90, 111
Ｙ	ＪＰ，９－５１５２０，Ａ（ソニー株式会社），１８．２月．１９９７（１８．０２．９７）（ファミリーなし）	1-7, 12-26, 28-56, 58-89, 91-110, 112-122
Ａ		8-11, 27, 57, 90, 111
Ｙ Ａ	ＪＰ，９－２８４７６３，Ａ（ソニー株式会社），３１．１０月．１９９７（３１．１０．９７）（ファミリーなし）	8, 9 1-7, 10-122
Ｙ Ａ	ＪＰ，９－３１２６２５，Ａ（ソニー株式会社），２．１２月．１９９７（０２．１２．９７）（ファミリーなし）	8, 9 1-7, 10-122
Ｙ Ａ	ＪＰ，１０－１２６３７１，Ａ（ソニー株式会社），１５．５月．１９９８（１５．０５．９８）（ファミリーなし）	8, 9 1-7, 10-122
Ａ	ＪＰ，７－２０２８８４，Ａ（ソニー株式会社），４．８月．１９９５（０４．０８．９５）（ファミリーなし）	1-122
Ａ	ＪＰ，８－２８９２７７，Ａ（ソニー株式会社），１．１１月．１９９６（０１．１１．９６）（ファミリーなし）	1-122
Ａ	ＪＰ，８－３４０５１４，Ａ（ソニー株式会社），２４．１２月．１９９６（２４．１２．９６）（ファミリーなし）	1-122
Ａ	ＪＰ，９－９２４１，Ａ（ソニー株式会社），１０．１月．１９９７（１０．０１．９７）（ファミリーなし）	1-122
Ａ	ＪＰ，９－４６６７２，Ａ（ソニー株式会社），１４．２月．１９９７（１４．０２．９７）（ファミリーなし）	1-122
Ａ	ＪＰ，９－４６６８１，Ａ（ソニー株式会社），１４．２月．１９９７（１４．０２．９７）（ファミリーなし）	1-122
Ａ	ＪＰ，９－２８４７６２，Ａ（ソニー株式会社），３１．１０月．１９９７（３１．１０．９７）（ファミリーなし）	1-122
Ａ	ＪＰ，９－３０７５４２，Ａ（ソニー株式会社），２８．１１月．１９９７（２８．１１．９７）（ファミリーなし）	1-122
Ａ	ＪＰ，９－３２２１６１，Ａ（株式会社エクシング），１２．１２月．１９９７（１２．１２．９７）（ファミリーなし）	1-122

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ９８／０３１２７

第Ⅰ欄　請求の範囲の一部の調査ができないときの意見（第１ページの１の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲 _____は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、

2．☐ 請求の範囲 _____は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☐ 請求の範囲 _____は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄　発明の単一性が欠如しているときの意見（第１ページの２の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲１－７、１２～１２２はデータエレメントの暗号化に関するものであり、請求の範囲８－１１はデータエレメントの時分割多重化時のバッファリングに関するものであり、これら２つの発明群が単一の一般的発明概念を形成するように関連している一群の発明であるとは認められない。

1．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☒ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。